Pubblicazione Trimestrale
ISSN: 2279-9737

Rivista di Diritto Bancario

dottrina
e giurisprudenza
commentata

Supplemento
Ottobre / Dicembre
2024

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

2024

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

NORME PER LA VALUTAZIONE E LA PUBBLICAZIONE

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

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

I contributi sono anonimizzati prima dell'invio ai valutatori.

Le schede di valutazione sono inviate agli autori previa anonimizzazione.

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

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

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

SEDE DELLA REDAZIONE

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

NICOLA M. F. FARAONE

IA e vigilanza prudenziale: alla ricerca di un nuovo equilibrio tra presidio dei rischi e trasformazione digitale dell'impresa bancaria*

1. *Introduzione (con una premessa di metodo)*

Il Regolamento sull'intelligenza artificiale ("AI Act" o anche il "Regolamento")[1] definisce i caratteri minimi dell'intelligenza artificiale ("IA"), riconosce nella trasparenza, "spiegabilità" e fiducia da parte dei consumatori europei[2] i "pilastri" di base su cui devono

* Il presente scritto costituisce una versione ampliata e aggiornata del contributo presentato al Convegno ADDE "Regolazione del rischio nel Diritto dei mercati finanziari" che si è svolto presso l'Università di Cagliari il 13 e 14 giugno 2024. Desidero ringraziare il Prof. Andrea Sacco Ginevri per gli spunti di riflessione e i commenti forniti in occasione della presentazione della prima versione del lavoro.

[1] 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) n. 2018/858, (UE) n. 2018/1139 e (UE) n. 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[2] Del resto, è, ormai, un dato acquisito che tutta la legislazione europea di recente introduzione intenda promuovere l'innovazione con una normativa che favorisca il mercato purché armonizzata con i valori europei, "disegnando", così, una sorta di limite di "ordine pubblico europeo" di direzione per il mercato e di protezione per le persone, volto a impedire che i diritti fondamentali possano essere pregiudicati nell'esercizio di attività economiche. Si rimanda, per un approfondimento, a V.

poggiare le "fondamenta" dell'attività dei fornitori e dei *deployer*, gradua gli obblighi sulla base della loro "rischiosità" sino al punto di vietare alcuni sistemi e modelli (se hanno, ad esempio, come oggetto o effetto il *social scoring* o le pratiche manipolative). Proprio perché non introduce un codice europeo sull'IA né tantomeno il Testo Unico della materia, è necessario analizzare il Regolamento "in controluce" "riempiendo i vuoti" e colmando le lacune interpretative con una lettura orientata della legislazione esistente[3].

Quest'operazione "ermeneutica" è tanto più imprescindibile, per le potenziali criticità e per la rilevanza sistemica che ne scaturisce, in caso di utilizzo di sistemi di IA nell'ambito del settore finanziario (da parte di istituzioni finanziarie o, comunque, nel contesto della prestazione di servizi finanziari).

FALCE, *Piattaforme di ecosistemi digitali. Scelte pro-concorrenziali*, in *Riv. dir. ind.*, 2022, IV-V-VI, 172. Anche al di fuori dei confini europei, l'effetto atteso è di elevare l'Unione a *standard* normativo nel mercato internazionale dell'IA, sulla scorta del famigerato "effetto Bruxelles" che, già con la normativa europea a tutela dei dati personali, ambisce a divenire piattaforma "attrattiva" di soluzioni tecnologiche di imprese extra-UE in concorrenza o in *partnership* con imprese europee. Si rimanda al celeberrimo contributo di A. BRADFORD, *The Brussels Effect: How the European Union Rules the World* (New York, 2020; online edn, Oxford Academic, 19 Dec. 2019.

[3] A titolo esemplificativo ma non esaustivo, si rimanda a V. FALCE (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Torino, 2023, *passim*; G. LEMME, *La transizione giuridica. La crisi del diritto di fronte alla sfida tecnologica*, Torino, 2023, 127; G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubb.*, 2022, 1087; per un profilo informatico (ancorché di tipo esplicativo) G. F. ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *Anal. Giur. Economia*, 2019, I, 10; T. E. FROSINI, *L'ordine giuridico del digitale*, in *Giur cost.*, 2023, II, 391; C. NOVELLI, F. CASOLARI, A. ROTOLO, M. TADDEO, L. FLORIDI, *Taking the AI risk seriously: a new assesment model for the AI Act*, in *AI & Society*, 2023; M. ALMADA, N. PETIT, *The EU AI Act: a medley of product safety and fundamental rights?*, in *Robert Schuman Centre for Advanced Studies Research Paper No. 2023/59*; T. SCHREPEL, *Decoding the AI Act: A Critical Guide for Competition Experts*, in *Amsterdam Law & Technology Institute Working Paper Series 2024*; L. FLORIDI, *On the Brussels-Washington Consensus About the Legal Definition of Artificial Intelligence*, in *Philosophy & Technology, 2023*; G. MALGIERI, F. PASQUALE, *From Transparency to Justification: Toward Ex Ante Accountability for AI*, in *Brooklyn Law School, Legal Studies Paper No. 712, Brussels Privacy Hub Working Paper, No. 33.*

Proprio a tutela degli investitori e della stabilità del sistema, non è un caso, quindi, che l'AI Act abbia riconosciuto la necessità di coordinare la vigilanza sull'intelligenza artificiale ("IA") e la vigilanza bancaria (anche prudenziale)[4].

La formula (forse abusata) che vuole il Regolamento come veicolo di diffusione (anche culturale) di un approccio orizzontale e basato sul rischio (i.e., esclusione dal commercio per i sistemi a rischio inaccettabile, requisiti minimi e piuttosto generali per i sistemi ad alto rischio e assenza di regolamentazione per i sistemi a basso rischio)[5] altro non è che la manifestazione tangibile della dialettica tra due interessi in gioco, che trovano nel settore finanziario uno "ponte" naturale e un punto di equilibrio inevitabile: lo sviluppo tecnologico, da un canto, e la tutela dei diritti fondamentali[6], dall'altro, in uno con la fiducia nei mercati finanziari e negli intermediari che vi operano[7].

[4] Da ultimo, v. Financial Stability Board, The Financial Stability Implications of Artificial Intelligence, 14 november 2024.

[5] Cfr., tra gli altri, G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Il Diritto dell'informazione e dell'informatica*, 2022, II, 303. La scelta si pone, d'altronde, in linea con i principi enunciati nel "Libro bianco sull'intelligenza artificiale", nel quale la Commissione evidenzia come: «*In linea di principio il nuovo quadro normativo per l'IA dovrebbe essere efficace nel raggiungimento dei propri obiettivi, senza tuttavia essere talmente prescrittivo da creare oneri sproporzionati, in particolare per le PMI. Per raggiungere tale equilibrio la Commissione ritiene opportuno seguire un approccio basato sul rischio*». Cfr. Commissione europea, *Libro bianco sull'intelligenza artificiale – un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final, Bruxelles, 19 febbraio 2020.

[6] Si veda, per un'introduzione, L. AMMANNATI, *Diritti fondamentali e* rule of law *per un'intelligenza artificiale*, in *Riv. trim. dir. econ.*, 2021, Suppl. n. III, 170.

[7] Per una lettura critica circa l'opinione comune secondo cui una regolamentazione più stringente dell'economia digitale comprometta inevitabilmente l'innovazione, pregiudichi il progresso tecnologico e "annacqui" le tutele, v. A. BRADFORD, *The False Choice Between Digital Regulation and Innovation*, in *Northwestern University Law Review*, Vol. 118, Issue 2, October 6, 2024. Come noto, tale approccio ideologico, sostenuto con forza dall'industria tecnologica, ha plasmato l'opinione pubblica negli Stati Uniti, dove la fiorente economia tecnologica del Paese è spesso associata a un convinto impegno per il libero mercato e per la *deregulation*. Anche il legislatore negli Stati Uniti ha tradizionalmente abbracciato questa prospettiva, ciò che spiega l'esitazione al di là dell'Oceano a regolamentare l'industria tecnologica.

Ciò chiarito – e superata la fase di *battage* mediatico legata all'*iter* approvativo del Regolamento[8] –, occorre interrogarsi circa i margini di adattamento del nuovo strumentario alla previgente normativa finanziaria e, in ultima istanza, vanno indagate specialmente le prospettive e i rischi di vigilanza.

2. *Una prima ricostruzione della tassonomia dei rischi emergenti nel settore finanziario*

2.1. *L'emersione del governo del rischio "tecnologico" nella gestione dell'impresa*

Allo sviluppo dell'intelligenza artificiale – consacrato nell'approvazione del Regolamento – e all'atteso incremento di produttività anche nel settore finanziario corrispondono, in parallelo, i rischi generati dal suo impiego.

[8] L'*iter* legislativo è stato piuttosto rapido. È stata, infatti, approvata da parte del Parlamento europeo e del Consiglio, secondo la procedura legislativa ordinaria, la proposta di Regolamento sull'AI Act, presentata dalla Commissione europea il 21 aprile 2021 (COM/2021/206 final 2021/0106(COD)). In esito ai triloghi (negoziati inter-istituzionali tra i rappresentanti di Parlamento europeo, Consiglio e Commissione per concordare il testo da sottoporre all'approvazione dei due co-legislatori), il 9 dicembre 2023, al termine di una sessione negoziale di tre giorni, è stato, infatti, raggiunto un accordo politico provvisorio, con l'obiettivo di approvare in via definitiva la nuova normativa entro la conclusione dell'attuale legislatura europea. L'accordo dovrà ora essere formalmente approvato dal Consiglio (a maggioranza qualificata), e dal Parlamento europeo (a maggioranza dei suoi componenti), al più tardi nella sessione del prossimo aprile. Il 2 febbraio il Comitato dei rappresentanti permanenti degli Stati membri presso l'UE (COREPER), massimo organo preparatorio dei lavori del Consiglio, ha approvato all'unanimità il testo dell'accordo del 9 dicembre. Prima dell'avvio dei negoziati, il Consiglio dell'UE, con un orientamento generale adottato all'unanimità il 6 dicembre 2022 e il Parlamento europeo con emendamenti approvati in plenaria (con 499 voti a favore, 28 contrari e 93 astensioni) il 14 giugno 2023 avevano definito le proprie posizioni. Effettivamente, il Parlamento europeo ha approvato lo scorso 13 marzo 2024 il Regolamento, frutto dell'accordo raggiunto con gli Stati membri nel dicembre 2023, con 523 voti favorevoli, 46 contrari e 49 astensioni. È stato, poi, pubblicato in Gazzetta Ufficiale dell'Unione europea il 12 luglio 2024 ed entrato in vigore lo scorso 1° agosto 2024.

L'emersione, nel dibattito dottrinale, della fortunata (e talvolta abusata) formula di "diritto privato regolatorio"[9] (o anche di diritto regolatorio[10]) ha accelerato la tendenza dei regolatori pubblici – già consolidatasi "sotto pelle" nell'ultimo ventennio – ad una più intensa "responsabilizzazione" degli operatori economici nell'attività di identificazione e gestione dei rischi. Si è elevato l'adozione di efficaci ed adeguati processi di misurazione preventiva e governo del rischio (il c.d. *risk management*) e di *compliance* normativa e regolamentare a dovere giuridicamente vincolante per gli esponenti apicali nel quadro dell'obbligo di adozione di adeguati assetti organizzativi e di controllo interno (anziché "degradarlo" a mera regola di condotta non prescrittiva e ancor meno "cogente" nell'operatività delle aziende)[11].

Dinnanzi alle istanze di tutela della "società del rischio"[12], le tappe sono state ben scandite e sono così riassumibili: dopo una prima fase di gestione del rischio che si giocava a livello del diritto penale e portata

[9] Una ricognizione dei significati e dell'ampiezza della formula è rinvenibile in R. NATOLI, *Il diritto privato regolatorio*, in *Rivista della Regolazione dei mercati*, 2020, I, 134 che allude all'uso, da parte dello Stato regolatore, del diritto privato in funzione di regolazione dei mercati e che si chiede se non sia già il tempo della definitiva torsione di questa formula in quella, più *tranchant*, di "Stato salvatore", citando G. NAPOLITANO, *Il nuovo Stato salvatore: strumenti di intervento e assetti istituzionali*, in *Giornale dir. amm.*, 2008, 1083, L. TORCHIA, *Politica industriale e regolazione*, in *Rivista della Regolazione dei mercati*, 2015, I, *passim*; M. CLARICH, *La "mano visibile" dello Stato nella crisi economica e finanziaria*, in *Rivista della Regolazione dei mercati*, 2015, II, 3.

[10] Più in generale, al di là delle nomenclature, A. GENTILI, *Il diritto regolatorio*, in questa *Rivista*, 2020, Suppl. I, 23 passa in rassegna, anche dal punto di vista storico, lo spirito del diritto regolatorio, le ragioni culturali e istituzionali all'origine della regolazione.

[11] Si veda, per un'introduzione al tema, S. CERRATO (a cura di), *Impresa e rischio. Profili giuridici del* risk management, Torino, 2019, *passim*. Più in generale, in ordine all'intrinseca immanenza di un «elemento di rischio» alla nozione di impresa fissata nell'art. 2082 c.c. cfr. F. CAVAZZUTI, *voce «Rischio d'impresa»*, in *Enc. del dir.*, Aggiornamento, IV, Milano, Giuffrè, 2000, 1093. Nel vigore del cod. di comm., C. VIVANTE, *I commercianti*, nel Tratt. dir. comm., I, Milano, Vallardi, 1934, 100, n. 61. ascriveva il rischio ai requisiti essenziali di ogni impresa.

[12] Un orizzonte che il sociologo tedesco Ulrich Beck ha codificato in una definizione fortunata, attualissima ed efficace: Risikogesellschaft, società del rischio, nel suo volume dal titolo, appunto, di: Risikogesellschaft: auf dem Weg in eine andere Moderne, Frankfurt am Main, 1986; più di recente, ID., Conditio humana. *Il rischio nell'età globale*, Bari, 2008.

avanti attraverso l'adozione di misure preventivo-cautelari volte a minimizzare i rischi noti e a gestire quelli ignoti, sul piano civilistico l'occasione per invertire la tendenza si è materializzata in occasione della revisione della disciplina dei mercati finanziari e delle società quotate (il pensiero va necessariamente all'art. 149 del Testo Unico Bancario ("TUF") che, imponendo, per la prima volta, ai sindaci un dovere di vigilanza sull'adeguatezza degli assetti organizzativi, amministrativi e contabili, indirettamente pone a livello normativo un dovere di adozione di essi, ed esige che la società quotata sia dotata di un sistema di controllo interno), che è stato, poi, generalizzato con la riforma del diritto societario del 2003 (artt. 2381 e 2403 c.c.), e che si è ulteriormente sedimentato con il D.lgs. 8 giugno 2001, n. 231 sulla responsabilità amministrativa degli enti (specialmente a seguito dell'incremento del catalogo dei "reati-presupposto").

Cifra comune di questa "moltiplicazione" normativa è l'emanazione di una legislazione primaria che contiene precetti specifici inerenti il c.d. *enterprise risk management*, cioè i metodi e i processi di gestione del rischio[13].

È in questo contesto che si inserisce lo studio dei problemi che pongono le nuove tecnologie basate su intelligenza artificiale[14].

Innanzitutto, su un piano più generale, l'utilizzo dell'IA ha avuto il merito di far affiorare la tematica del rischio "tecnologico" come una forma separata di rischio, in aggiunta al rischio operativo come più tradizionalmente inteso, che ben potrebbe originare, dal punto di vista

[13] Basti pensare al Codice della crisi d'impresa e dell'insolvenza (D.Lgs. 12 gennaio 2019, n. 14) che ha individuato due pilastri su cui fondare la prevenzione dell'insolvenza: (i) gli obblighi organizzativi, per cui ogni tipo di azienda è tenuta a dotarsi di "assetti organizzativi adeguati alla rilevazione tempestiva della crisi" e a predisporre misure atte a contrastarla; e (ii) gli strumenti di allerta, in grado di far emergere precocemente gli indizi della crisi e dello stato di difficoltà in cui versa l'impresa (il c.d. *early warning*).

[14] Si rimanda, per un'introduzione ai problemi, a V. FALCE (a cura di), Financial Innovation *tra Disintermediazione e Mercato*, Giappichelli, Torino, 2021, *passim*; ID., Data Strategy *e intelligenza artificiale*, in M. PASSALACQUA (a cura di), *Diritti e mercati nella transizione ecologica e digitale*, Padova, 2021; A. SCIARRONE ALIBRANDI, *Innovazione tecnologica e regolazione dei mercati*, in R. LENER, G. LUCHENA, C. ROBUSTELLA (a cura di), *Mercati regolati e nuove filiere di valore*, Torino, 2021, 5; M. PELLEGRINI, *Innovazione tecnologica e diritto dell'economia*, in *Riv. trim. dir. econ.*, 2019, IV, 40.

soggettivo, da una singola istituzione, così come dalle interconnessioni tra diverse entità[15].

2.2. *Le tipologie di rischi "tecnologici" nell'utilizzo dell'IA*

A questo punto, non è senza interesse tentare di "sistematizzare" e proporre una tassonomia dei rischi tecnologici da utilizzo di IA[16].

Di là da quello reputazionale (senza dubbio rilevante, ma ultroneo rispetto al perimetro della presente analisi), il primo *genus* di rischio tecnologico cui l'impresa bancaria è soggetta nella doppia fase della selezione dell'infrastruttura cibernetica di cui dotarsi e dell'utilizzo in sicurezza del sistema di IA è quello *cyber*[17].

Innanzitutto, in sede di contrattualizzazione dell'"impalcatura *cyber*", è evidente che la concentrazione del mercato dei fornitori di tecnologia e la mancanza di alternative prontamente accessibili possano determinare un aumento dei rischi operativi e delle esternalità negative tipiche del "*too-big-to-fail*"[18]. Non sfugge, infatti, che, al crescere della

[15] Per una lettura introduttiva all'argomento ma "precorritrice dei tempi", cfr. R.P. BUCKLEY, D.W. ARNER, D.A. ZETZSCHE, E. SELGA, *The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk*, in "UNSW Law Research Paper No. 19-89, European Banking Institute Working Paper 2019/54, University of Luxembourg Law Working Paper 2019-009", University of Hong Kong Faculty of Law Research Paper No. 2019/112.

[16] Si rimanda al contributo di S.A. CERRATO, F. CULASSO, E. CROCCO, "Handle with care". *Per una governance dell'intelligenza artificiale nell'impresa: rischi, tecniche di gestione, assetti cibernetici*, in *Riv. soc.*, 2023, II-III, 371.

[17] Si veda per un commento Basel Committee on Banking Supervision. (2018a). Cyber-resilience: Range of practices. Bank for International Settlements. Più di recente, si veda un'interessante contributo pubblicato tra i *paper* della Bank for International Settlements (BIS) che mette in relazione i rischi *cyber* dal punto di vista bancario con i rischi nascenti (e ancora da esplorare) dell'IA generativa: I. ALDASORO, S. DOERR, L. GAMBACORTA, S. NOTRA, T. OLIVIERO, D. WHYTE, *Generative artificial intelligence and cyber security in central banking*, BIS Papers No. 145, May 2024, disponibile al *link*: https://www.bis.org/publ/bppdf/bispap145.htm. Si veda, inoltre, il recente intervento della Vice Direttrice Generale della Banca d'Italia, A. PERRAZZELLI, *Le interconnessioni tra Intelligenza Artificiale, Cloud e Cyber nel settore finanziario*, Cetif Summit. Innovation Trends in Finance 2024, 5 giugno 2024.

[18] Vien da sé che non si fa riferimento, con una formula siffatta, all'impossibilità per i governi di astenersi da un salvataggio di un intermediario bancario avente valenza "sistemica" senza scatenare contraccolpi a livello globale, ma, piuttosto, si

sofisticatezza della tecnologia utilizzata e/o immessa sul mercato, maggiori saranno gli investimenti richiesti e, di conseguenza, minore il numero di imprese in grado di svilupparla e implementarla, fino all'eventualità estrema che si possa contare su un solo produttore.

È verosimile, dunque, il pericolo di trovarsi senza reali alternative (o con un numero molto ristretto di opzioni), rendendosi, in questo modo, fortemente dipendenti dal produttore, sia nel breve termine (politica dei prezzi, adattabilità alle esigenze concrete) che in un orizzonte temporale più ampio (condizioni di rinnovo di licenze, *release* di nuove versioni, ecc.)[19].

Relativamente al tema della sicurezza, il ricorso alle nuove tecnologie ha condotto alla moltiplicazione anche "qualitativa" dei rischi, se è vero che l'interconnessione globale rende potenzialmente aggredibile e *hackerabile* dall'esterno la rete aziendale in mancanza di idonee protezioni tramite *firewalls* e di sistemi anti-intrusione. Senza contare che si è diffusa, in luogo di quella fisica, l'archiviazione digitale dei documenti tramite conservazione di *file* in *cloud* la cui sottrazione, criptazione per fini estorsivi o distruzione o dispersione è all'ordine del giorno[20]. Ebbene, questa prospettiva è stata presa in esame dall'AI Act che è giunto ad imporre ai produttori di sistemi cibernetici (che siano ad alto rischio) di dotarsi di «*soluzioni tecniche volte a garantire la cybersicurezza*» «*adeguate alle circostanze e ai rischi pertinenti*», includendo anche «*misure volte a prevenire, accertare, rispondere, risolvere e controllare gli attacchi che cercano di manipolare il set di dati di addestramento* ("avvelenamento dei dati", o anche il c.d. "data poisoning") *o i componenti pre-addestrati utilizzati nell'addestramento* ("avvelenamento dei modelli", o anche "model poisoning"), *gli* input *progettati in modo da far sì che il modello commetta un errore* ("esempi antagonistici", anche definiti come "adversarial examples" o "evasione dal modello", anche definiti come "model evasion"), *gli attacchi alla*

vuole evocare una tendenza irreversibile dei mercati, vale a dire l'integrazione dei sistemi (anche dei fornitori "esterni" di soluzioni tecnologiche). Per qualche spunto, di ordine storico, si veda, in ogni caso, Financial Stability Board (FSB), Evaluation of the Effects of Too-Big-To-Fail Reforms. Final Report, 1 April 2021.

[19] S.A. CERRATO, F. CULASSO, E. CROCCO, *op. cit.*, 371 lo definisce rischio di "monopolio" o di "oligopolio" tecnologico.

[20] Così, S.A. CERRATO, F. CULASSO, E. CROCCO, *ibidem*, che fanno parola di rischio di "corruzione" di dati.

riservatezza o i difetti del modello, che potrebbero condurre a decisioni dannose»[21].

Un'ulteriore categoria di rischi da "soppesare" è quella legata all'incremento incessante delle attività in *outsourcing*[22].

Lo sviluppo di soluzioni tecnologiche beneficia, infatti, di enormi economie di scala, che rendono conveniente per il singolo operatore ricorrere a *provider* esterni, i quali, tuttavia, tendono ad avere dimensioni molto più ampie rispetto a quelle del soggetto servito e a operare in mercati molto concentrati[23].

L'esperienza maturata ha dimostrato che, sino a oggi, questo rischio è sotto controllo e desta preoccupazioni limitate, dal momento che il rapporto tra banche e imprese tecnologiche "terze" sta evolvendo

[21] Cfr. Art. 15 del Regolamento.

[22] Secondo EBA, Relazione finale sugli orientamenti in materia di esternalizzazione (EBA/GL/2019/02), 25 febbraio 2019, 5, la nozione di esternalizzazione deve intendersi come «*un accordo di qualsiasi forma tra un ente, un istituto di pagamento o un istituto di moneta elettronica e un fornitore di servizi in base al quale quest'ultimo svolge un processo, un servizio o un'attività che sarebbe altrimenti svolto/a dall'ente, dall'istituto di pagamento o dall'istituto di moneta elettronica stesso*». Per una considerazione generale sul fenomeno dell'*outsourcing*, cfr. A. SACCO GINEVRI, *Esternalizzazione* (outsourcing), in G. FINOCCHIARO, V. FALCE (a cura di), Fintech*: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019, 205; M. CAROLI, A. VALENTINO, *La strategia di «outsourcing»*, in *Analisi giur. econ.*, 2011, II, 255; P. SODA, *La regolamentazione dell'*outsourcing *nel settore finanziario: orientamenti In Italia, Europa e Stati Uniti*, in *Bancaria*, 2006, X, 43; M. MAUGERI, *Esternalizzazione di funzioni aziendali e «integrità» organizzativa nelle imprese di investimento*, in *Banca, borsa, tit. cred.*, 2010, IV, 439; L. ENRIQUES, W.G. RINGE, *Bank-fintech partnerships, outsourcing arrangements and the case for a mentorship regime*, in *Capital Markets Law Journal*, 2020, IV, 374; V. LEMMA, J.A. THORP, *Sharing Corporate Governance: The Role of Outsourcing Contracts in Banking*, in *Law and Economics Yearly Review*, 2014, III, 357; S. CASAMASSIMA, M. NICOTRA (a cura di), *L'*outsourcing *nei servizi bancari e finanziari*, Padova, 2021, *passim*; L. SPITALERI, *L'*outsourcing *nei servizi bancari e finanziari, profili di* governance *e prospettive di vigilanza*, in *Riv. trim. dir. econ.*, 2023, Suppl. II, 111.

[23] Peraltro, in data 3 giugno 2024, la BCE avvia oggi una consultazione pubblica (che terminerà il 15 luglio 2024) sulla c.d. *ECB Guide on outsourcing cloud services to cloud service providers*. Inoltre, la BCE ha individuato diverse vulnerabilità negli accordi di esternalizzazione informatica delle banche durante il processo di revisione e valutazione prudenziale 2023. Di conseguenza, la gestione del rischio di terzi, compreso l'*outsourcing* del *cloud*, continua a rimanere in cima alla lista delle priorità di vigilanza della BCE per il periodo 2024-2026.

strutturalmente da un piano di competizione diretta a uno di collaborazione[24].

A fronte di ciò, si pongono, ciononostante, per il singolo intermediario, questioni di "forza contrattuale", che possono tradursi in minore capacità di ottenere condizioni economiche favorevoli, scarsa personalizzazione del rapporto e, più in generale, ridotta attenzione da parte del fornitore, con potenziali riflessi negativi sulla qualità dei prodotti e servizi offerti[25], nonché sulla competitività[26].

Sullo sfondo non si può ignorare il rischio di distorsione del processo decisionale causato dall'impatto della tecnologia nella vita della società. Allo stato, nulla fa ipotizzare che applicazioni di IA possano, in tempi brevi, assumere un ruolo formale di componente di un organo amministrativo o di un *board* e affiancare gli amministratori "umani" nei consigli di amministrazione (senza contare i limiti tecnologici che ancora ostano ad un efficiente impiego dell'IA in sostituzione di

[24] Tale tendenza è confermata dagli esiti della recente indagine della Banca d'Italia sul settore Fintech, finalizzata ad analizzare la trasformazione digitale e le prospettive di innovazione del nostro sistema finanziario. Cfr. Banca d'Italia, *Indagine Fintech nel sistema finanziario italiano*, aprile 2024.

[25] Di recente, ESMA ha sottolineato, in una dichiarazione (*public statement*) pubblicata lo scorso 30 maggio 2024, come sussista un rischio inerente anche per le imprese che utilizzano l'IA quando forniscono servizi di investimento ai clienti al dettaglio, in ambito MIFID II. A tal proposito, quando utilizzano l'IA, ESMA si aspetta che le imprese rispettino i requisiti della MiFID II, in particolare per quanto riguarda: gli aspetti organizzativi, la condotta aziendale, l'obbligo normativo di agire nel miglior interesse del cliente. Si veda ESMA, Public Statement. On the use of Artificial Intelligence (AI) in the provision of retail investment services, 30 May 2024, ESMA35-335435667-5924.

[26] Si veda, da ultimo, Banca d'Italia, Segnalazione in materia di esternalizzazione di funzioni aziendali per gli intermediari vigilati, provvedimento del 31 maggio 2023 (Delibera 166/2023). Merita segnalare, inoltre, gli Orientamenti dell'ESMA in materia di esternalizzazione a fornitori di servizi cloud (ESMA50-164-4285) del 10 maggio 2021. Sul punto il principio generalmente accolto è il seguente: "*esternalizzazione sì, impunità no*". I principi guida in materia di *outsourcing* nei servizi finanziari sono stati enunciati per la prima volta dal Comitato di Basilea nel 2005 (BIS, Outsourcing in Financial Services, February 2005) sottolineandosi, tra l'altro, la necessità che l'intermediario assicuri il corretto e puntuale svolgimento delle attività esternalizzate, tanto nei confronti del regolatore quanto dei clienti, senza che in alcun modo possa venir meno la responsabilità del committente.

amministratori umani)[27]. Ma ben più concreta è la prospettiva che l'IA supporti e arricchisca le capacità decisionali dell'organo amministrativo[28] o fornisca supporto istruttorio nell'adozione delle decisioni relative alla gestione dell'impresa[29], senza arrivare al punto

[27] Si rimanda, tra gli altri, ai contributi di A. SACCO GINEVRI, *Intelligenza artificiale e* corporate governance, in R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022, 429; ID., *Ancora su intelligenza artificiale e* corporate governance, in *Riv. trim. dir. econ.*, 2021, III (Suppl. II), 343; G.D. MOSCO, Roboboard. *L'intelligenza artificiale nei consigli di amministrazione*, in AGE, 2019, I, 247; M.L. MONTAGNANI, *Il ruolo dell'intelligenza artificiale nel funzionamento del consiglio di amministrazione delle società per azioni*, Milano, 2021, 89; ID., *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, in *Pers. Merc.*, 2020, II, 67; F. MÖSLEIN, *Robots in the Boardroom: Artificial Intelligence and Law*, in W. BARFIELD, U. PAGALLO (a cura di), *Research Handbook on the Law of Artificial Intelligence*, Cheltenham, 2018; N. ABRIANI, G. SCHNEIDER, *Il diritto societario incontra il diritto dell'informazione. IT,* Corporate governance e Corporate Social Responsibility, in *Riv. soc.*, 2020, V-VI, 1374; U. TOMBARI, *Intelligenza artificiale e* corporate governance *nella società quotata*, *ivi*, 1431.

[28] M.L. MONTAGNANI, M.L. PASSADOR, *Il consiglio di amministrazione nell'era dell'intelligenza artificiale: tra* corporate reporting, *composizione e responsabilità*, in *Riv. Soc.*, 2021, I, 121. Una tesi sulla quale si è convogliato un consenso generalizzato è quella che vede nell'IA un (eccellente) sostituto degli attori umani nell'adempimento della maggior parte delle operazioni (in senso stretto) amministrative (se si vuole, più routinarie), ma non ancora in grado di assolvere pienamente quelle diverse attività che richiederebbero "judgment work": v. H. BIRD-NATANIA LOCKE, *The corporate board in an age of collaborative intelligence and complex risk*, in *Technology and Corporate Law. How Innovation Shapes Corporate Activity*, Edward Elgar, 2021, 47. Si veda ancora F. PACILEO, *"Scelte d'impresa" e doveri degli amministratori nell'impiego dell'intelligenza artificiale*, in *Riv. Dir. Soc.*, 2022, III, 539 e spec. 573 e 576.

[29] Sul punto, diffusamente, L. ENRIQUES, A. ZORZI, *Intelligenza artificiale e responsabilità degli amministratori*, in N. ABRIANI, R. COSTI (a cura di), *Diritto societario, digitalizzazione e Intelligenza Artificiale*, Quaderni di Giurisprudenza Commerciale, Milano, 187. L'utilizzo dei sistemi di IA è orientato, pertanto, a formulare "previsioni". Esempi applicativi possono consistere, a titolo esemplificativo, nel predire l'esito di una futura controversia tra la società ed un fornitore e/o un cliente, oppure prefigurare le conseguenze, anche sanzionatorie, partendo da una sequenza di dati ipotizzati. Chiaramente, secondo gli A., individuare quale operazione realizzi al meglio l'interesse sociale è un compito che, data l'ampia discrezionalità che vi si collega, mal si attaglia ad un decisore algoritmico. Pertanto,

che ad esso si affidi la scelta del c.d. *corporate purpose*[30]. E, difatti, con la nascita e lo sviluppo delle tecnologie più nuove e avanzate, è stata coniata l'espressione *Corporate Technology* o *CorpTech* per indicare «*the use of distributed ledgers, smart contracts, Big Data analytics, AI and machine learning in the corporate context*»[31], che è, senz'altro, una formula efficace a livello descrittivo perché condensa in un concetto unitario l'adattabilità delle varie soluzioni tecnologiche all'impresa[32], ma ancora non sufficientemente specifica se con essa si vuole declinare uno statuto tecnologico della società.

Allargando la prospettiva adottata per questa sottocategoria di rischi tecnologici, il ricorso all'AI che "prende parte" all'attività gestoria pone criticità in punto di *accountability*, vale a dire di capacità di giustificazione (e conseguente assunzione di responsabilità) per le scelte adottate. Il rischio che ci si trova dinnanzi è quello dell'assenza

sempre a detta degli A., se si ipotizzasse di delegare all'algoritmo una decisione discrezionale, occorrerebbe rendere espliciti tanto lo scopo quanto i criteri di ponderazione delle decisioni.

[30] U. TOMBARI, *Intelligenza Artificiale, interesse sociale e sostenibilità nei codici di* corporate governance *e nella prassi societaria,* in N. ABRIANI, R. COSTI (a cura di), *ivi*, 332.

[31] L. ENRIQUES, D.A. ZETZSCHE, *Corporate Technologies and the Tech Nirvana Fallacy*, ECGI Working Paper, 2020, e in Hastings L. J., 2020, 59. L'espressione è stata, poi, ripresa da pressoché tutti gli studiosi che si sono cimentati sul terreno della cibernetica societaria: fra gli altri, N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, 2021, *passim*, i quali utilizzano, altresì, l'espressione cibernetica societaria come «*espressione riassuntiva della nuova* governance *dell'era algoritmica*» (*ivi*, 19); N. ABRIANI, *Intelligenza artificiale e diritto delle società: nuovi doveri e responsabilità degli amministratori*, in *Riv. dir. impr.*, 2022, I, *passim*.

[32] Com'è noto, questo processo ha subito un'evidente accelerazione in tempo di emergenza pandemica da Covid-19 allorquando l'utilizzo della tecnologia in ambito societario ha sconvolto gli assetti organizzativi delle imprese, non solo bancarie. L'esempio emblematico è stato rappresentato dalla valorizzazione di forme di partecipazione assembleari basate su modalità telematiche e virtuali, utilizzando strumenti di dialogo a distanza e di voto elettronico e anche a costo di sacrificare i tradizionali diritti dei soci di minoranza (fra cui quello di prender parte all'assemblea annuale degli azionisti) sull'altare della tutela della salute e della sicurezza personale. Ci si riferisce ai ben noti esempi della garanzia SACE (cfr. art. 1, D.L. 8 aprile 2020 n. 23 – c.d. "Decreto Liquidità" – conv., con modificazioni, dalla L. 5 giugno 2020 n. 40) e del c.d. "Patrimonio Rilancio" (cfr. art. 27, D.L. 19 maggio 2020 n. 34 - c.d. "Decreto Rilancio" – conv., con modificazioni, dalla L. 17 luglio 2020 n. 77).

di spiegabilità e trasparenza di queste applicazioni IA (c.d. "*black box dilemma*")[33] che, ricevuti gli *input*, restituiscono la risposta senza che sia intellegibile il percorso logico che ha condotto a tale risultato[34].

Al di là del tentativo di approntare appositi presidi di trasparenza degli algoritmi[35] e di investire nel rafforzamento delle competenze tecnologiche dei componenti degli organi di amministrazione e di controllo[36], rimane fermo e indifferibile il "fattore umano" nella determinazione dei fini assegnati all'AI all'interno del processo

[33] Così, su tale definizione, G. PAVLIDIS, *Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI*, in *Law, Innovation and Technology*, 2024, I, 293; J. BURRELL, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, in *Big Data & Society*, 2016, III, 1; D. CASTELVECCHI, *Can We Open the Black Box of AI?*, in *Nature*, 2016, 538, 21; W. VON ESCHENBACH, *Transparency and the Black Box Problem: Why We Do Not Trust AI*, in *Philosophy & Technology*, 2021, 34, 1607.

[34] Tale problema, che si scontra, come segnalato da M.L. MONTAGNANI, *Intelligenza artificiale e* governance *della "nuova" grande impresa azionaria: potenzialità e questioni endoconsiliari*, in *Riv. soc.*, 2020, IV, 1003, con l'esistenza di privative sugli algoritmi assicurate dalla vigente legislazione sui segreti commerciali (Dir. 2016/943, recepita in Italia con D.Lgs. n. 63/2018), è stato all'attenzione del legislatore europeo che nel Regolamento impone, fra l'altro, un obbligo di progettazione e sviluppo dei sistemi di AI ad alto rischio «*in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai fornitori e agli utenti di comprendere ragionevolmente il funzionamento del sistema*» (Art. 13). La categoria dei sistemi ad alto rischio include un esteso numero di possibili tecnologie cibernetiche (art. 6 e All. III) delle quali tuttavia solo un numero limitato possono essere immaginate di supporto all'*iter* decisionale di un organo amministrativo.

[35] In questo senso, si segnala la Proposta di Direttiva sulla responsabilità da intelligenza artificiale del 28 settembre 2022, COM(2022) 496 final 2022/0303(COD) nella quale si stabilisce che gli Stati debbono assicurare che l'autorità giudiziaria competente possa emettere, a richiesta di chi lamenti un plausibile pregiudizio derivante da utilizzo di intelligenza artificiale ad alto rischio, ordini di esibizione di informazioni rilevanti (art. 3, par. 1), sia pure nei limiti di quanto sia necessario e proporzionato per le esigenze di difesa di chi si dichiari danneggiato. Viene, inoltre, previsto che in caso di inottemperanza all'ordine, l'autorità giudiziaria «*shall presume the defendant's non-compliance with a relevant duty of care*».

[36] Oltre che nell'implementazione nella struttura organizzativa dell'impresa di uffici dedicati al monitoraggio e alla *compliance* dell'IA, dotandoli di protocolli e procedure ben delineate: si fa, infatti, parola di costruzione di un «*sistema di assetti cibernetici d'impresa*» (così, S.A. CERRATO, F. CULASSO, E. CROCCO, *op. cit.*, 371).

decisionale[37], caricando di nuovi contenuti i doveri di *monitoring* e, soprattutto, di *advisory* degli organi gestori[38].

2.3. *Il futuro* game-changer*: il Regolamento DORA*

Il rischio tecnologico, nel settore finanziario, diventa fonte, così, di rischio "sistemico"[39], al punto da dover fronteggiare profili di resilienza operativa e l'incremento degli incidenti operativi e degli attacchi

[37] Così si esprime N. ABRIANI, *Le categorie della moderna cibernetica societaria tra algoritmi e androritmi: "fine" della società e "fini" degli strumenti tecnologici*, in *Giur. Comm.*, 2022, V, 743, secondo cui «[c]*ome in altri campi da tempo noti – si pensi alla* policy *sulle remunerazioni, ma soprattutto a quella sull'*outsourcing, *che presenta molti profili di contiguità* […] *– il consiglio di amministrazione è chiamato a elaborare anche qui una* policy *rigorosa, che si iscrive nel quadro della più generale definizione della natura e del "livello di rischio compatibile con gli obiettivi strategici della società"* […]*: una regolamentazione che andrà ispirata all'etica della responsabilità e al principio di precauzione, i quali vengono a rivestire un peculiare rilievo in un ambito, come quello delle nuove tecnologie, nel quale i mezzi codeterminano e riconfigurano i fini* […]». Per un contributo "tradizionale", si v. D.A. ZETZSCHE, A.W. DOUGLAS, R.P. BUCKLEY E B. TANG, *Artificial Intelligence in Finance: Putting the Human in the Loop*, in CFTE Academic Paper Series: Centre for Finance, Technology and Entrepreneurship, n. 1, University of Hong Kong Faculty of Law Research Paper No. 2020/006.

[38] S.A. CERRATO, F. CULASSO, E. CROCCO, *op. cit.*, 371 richiamano l'attenzione sull'opzione di implementare «*sistemi di revisione o di* second opinion *umani o virtuali che consentano di testare la misura della* path dependency *dell'AI*». Si veda, inoltre, anche per gli ampi riferimenti bibliografici, F. CAPRIGLIONE, A. SACCO GINEVRI, *Metamorfosi della* governance *bancaria*, Torino, 2019, spec. 297. Secondo A. SACCO GINEVRI, *Intelligenza artificiale e* corporate governance, cit., 424, «*se è vero che la disciplina societaria è la veste organizzativa dell'impresa, l'utilizzo sempre più diffuso dell'intelligenza artificiale nei procedimenti aziendali favorirà un'evoluzione darwiniana della s.p.a. verso una accresciuta standardizzazione strutturale. Il tutto riservando alla sensibilità umana il potere e la responsabilità di pianificare l'alta strategia aziendale, con il compito di occuparsi delle questioni principali e la possibilità di concentrare attenzione e sforzi su aspetti di importanza fondamentale per l'impresa*».

[39] ESRB, Report – Systemic cyber risk, February 2020 e, da ultimo, ESRB, Advancing macroprudential tools for cyber resilience – Operational policy tools. April 2024. A review of national and pan-European frameworks, entrambi disponibili all'indirizzo: www.esrb.europa.eu.

cibernetici. Motivo per cui, già da diverso tempo (a partire dal 2018[40]), le istituzioni europee hanno avviato un percorso di riflessione culminato, a metà 2022, con l'approvazione di una normativa strutturata per il settore finanziario, il Regolamento sulla Digital Operational Resilience ("DORA")[41], la cui applicabilità è stata differita al 17 gennaio 2025 e da cui discenderà l'introduzione di poteri di *oversight* sulle "terze parti" ritenute critiche, nonché l'esigenza di rafforzare i presidi interni di banche e intermediari[42].

Esso mira, con un *risk-based approach*, a rafforzare la resilienza informatica delle entità finanziarie individuate, creando un quadro normativo comprensivo dei requisiti sulla gestione dei rischi informatici, sulla segnalazione degli incidenti informatici e sui test di resilienza operativa digitale. Il DORA contiene anche disposizioni sulla gestione dei rischi informatici derivanti da terzi, al fine di rispondere alle criticità in tema di integrazione tra "attori" del mondo finanziario e terze parti. Trascurando le disposizioni di dettaglio, che esulano dal perimetro di questo scritto[43], si segnala che le entità finanziarie che

[40] COMMISSIONE EUROPEA, Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo, 2018. Inoltre, alcune disposizioni previste ora dal DORA erano già applicate al settore finanziario sotto forma di linee guida: cfr. EBA, Guidelines on ICT and Security Risk Management.

[41] Regolamento (UE) 2022/2554 del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, GU L 333 del 27.12.2022, p. 1-79.

[42] Si rimanda al recentissimo contributo della Banca d'Italia che, lo scorso 23 dicembre 2024, ha pubblicato una comunicazione al mercato in materia di sicurezza ICT, richiamando l'attenzione degli intermediari direttamente vigilati sui profili della resilienza operativa digitale e del rischio ICT. Tale comunicazione richiama documento di analisi "*Digital resilience in the Italian financial sector: evidences from the supervisory incident reporting framework*" pubblicato da Banca d'Italia lo scorso 23 ottobre 2024 e che si basa sulle segnalazioni dei gravi incidenti operativi o di sicurezza che banche, istituti di pagamento e istituti di moneta elettronica hanno trasmesso tra il 2020 ed il 2023 alla Banca d'Italia ai sensi delle disposizioni di vigilanza.

[43] Per ulteriori approfondimenti, C.P. BUTTIGIEG, B. BRUNELLI ZIMMERMANN, *The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision*, in ERA Forum, 2024, 25:11-28; D. CLAUSMEIER, *Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)*, in *International Cybersecurity*

hanno stipulato accordi contrattuali per l'utilizzo di servizi ICT rimangono sempre pienamente responsabili dell'adempimento di tutti gli obblighi previsti dal DORA e dalla normativa finanziaria applicabile.

L'aspetto più interessante è dato dal fatto che DORA introduce un quadro di sorveglianza per i fornitori di servizi terzi critici nel settore ICT. Taluni fornitori terzi individuati dal Regolamento, in quanto particolarmente rilevanti in termini di impatto sistemico, di insostituibilità e di grado di dipendenza delle entità finanziarie, sono così sottoposti a speciale vigilanza da parte delle autorità di supervisione. Ciò segna una storica apertura alla vigilanza finanziaria di prestatori di servizi informatici non finanziari[44].

Law Review, 2023, 79. Cfr. anche S. KOURMPETIS, *Management of ICT Third Party Risk Under the Digital Operational Resilience Act*, in L. BÖFFEL, J. SCHÜRGER (eds), *Digitalisation, Sustainability, and the Banking and Capital Markets Union*, London, 2023, 211.

[44] In questa prospettiva, tenuto conto che il DORA costituisce un tassello importante verso l'inclusione dei sistemi di IA sviluppati da terzi nel perimetro della vigilanza finanziaria, la sfida è proprio quella di "affinare" la vigilanza sulle applicazioni di IA realizzate direttamente da soggetti non regolamentati per lo svolgimento di attività *de facto* finanziarie. A questo proposito, si confermerà ineludibile la necessità di definire un protocollo di collaborazione tra Comitato europeo per l'intelligenza artificiale e le ESAs (EBA, ESMA, EIOPA) per la vigilanza dei sistemi di IA utilizzati da operatori bancari (anche) "non istituzionali" e che forniscono servizi "non core". Esemplificativo di questa attenzione verso gli operatori di mercato non sottoposti a vigilanza e non regolamentati è la recente Legge 5 marzo 2024, n. 21 (c.d. Legge Capitali), che, introducendo una serie di modifiche al Testo Unico della Finanza e al Codice civile (in linea con le indicazioni del Rapporto OCSE del 2020 sul mercato dei capitali italiano e nel Libro Verde del MEF del 2022) intende perseguire l'obiettivo di rendere più efficiente l'accesso e la permanenza delle imprese sul mercato dei capitali, aumentandone la competitività. Tra le altre cose, si introduce una disciplina di favore e una serie di semplificazioni normative per le PMI (raddoppiando da 500 milioni a un miliardo di euro la soglia per quelle emittenti azioni quotate). Si verrà a creare, quindi, un doppio binario anche tra soggetti bancari "vigilati" e operatori non regolamentari, fornitori di servizi alle prime, che godranno di una disciplina semplificata, quantomeno per le procedure di quotazione e per le emissioni obbligazionarie e dei titoli di debito.

3. *Regolazione, supervisione,* governance*: una dialettica da ripensare*

Il ricorso da parte delle imprese bancarie alle tecnologie per automatizzare e "scalare" i processi interni e per migliorare e supportare la *compliance* normativa ha condotto alla "germogliazione" di nuovi termini (ormai abusati e sdoganati). Ci si riferisce alle definizioni di *RegTech* e di *SupTech*, che, benché talvolta usate in maniera promiscua[45], si differenziano in ciò, che la prima è volta a consentire agli intermediari finanziari di sviluppare e acquisire tecnologie per rendere più efficiente la *compliance* mentre la seconda è finalizzata a permettere alle Autorità di vigilanza l'uso di tecnologie abilitanti per facilitare la vigilanza e l'*enforcement*[46].

[45] Secondo A. PERRONE, *La nuova vigilanza* Reg Tech *e capitale umano*, in *Banca borsa tit. cred.*, 2020, IV, 516 ss. «[p]*ur essendo riferibile a una pluralità di ambiti, l'espressione* regulatory technology (RegTech) *è abitualmente utilizzata per identificare l'applicazione della tecnologia all'attività di* compliance *e di vigilanza nel sistema finanziario. Con maggiore precisione, il termine risulta talora utilizzato con esclusivo riguardo all'attività di* reporting *e* compliance *da parte dei soggetti vigilati, valendo per l'attività di vigilanza delle competenti autorità la più puntuale espressione* supervisory technology (SupTech). *L'uso promiscuo del termine RegTech è, nondimeno, il più diffuso, così da essere giustificato il suo impiego con riferimento a entrambi i fenomeni*». Per una rassegna dei diversi usi semantici dell'espressione, V. COLAERT, *RegTech as a response to regulatory expansion in the financial sector* (March 2017), in www.ssrn.com; sul punto v. anche A. YANG, C.Y. TSANG, *RegTech and the New Era of Financial Regulators: Envisaging More Public-Private-Partnership Models of Financial Regulators*, in U. Pa. J. Bus. L., 2018, Vol. 21, Issue 2, 354; L. ENRIQUES, *Financial Supervisors and Regtech: Four Roles and Four Challenges*, in *Revue Trimestrielle De Droit Financier*, 2017.

[46] Il termine SupTech, coniato solo nel 2017 (cfr. R. MENON, "Singapore fintech journey 2.0", remarks at the Singapore Fintech Festival, Singapore, 15 November 2017), faceva riferimento a un mercato ancora molto "acerbo" a quel tempo mentre alcuni fra i primi riferimenti agli strumenti RegTech si rinvengono, a livello europeo, in un documento dell'ESMA del 28.2.2019, dopo poco seguito da alcune indicazioni elaborate nel Final Report dell'Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), ove si auspicava la messa a punto da parte della Commissione, in cooperazione con le Autorità di vigilanza e con altre autorità competenti in materia (fra cui il Financial Stability Board, a sua volta intervenuto sul punto con un Report nel 2020: cfr. Financial Stability Board, The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions, 2020), di un'agenda completa e ambiziosa a supporto dell'adozione di sistemi RegTech e SupTech nel settore finanziario. Si veda ancora EBA, Analysis of RegTech in the EU Financial Sector,

Tale proliferazione lessicale è un sintomo, però, di qualcosa di più profondo, che disvela una crisi progressiva della regolazione come tradizionalmente intesa[47].

Il "ritardo" strutturale della regolamentazione rispetto al mercato, la sua conseguente esposizione a una rapida obsolescenza, la concentrazione del mercato derivante dall'impossibilità per gli intermediari minori di sostenere i costi derivanti da una regolamentazione sempre più complessa hanno reso urgente e non ulteriormente rinviabile la domanda se non sia la regolamentazione a dover "cambiare pelle" (e non, all'opposto, la costosa attività di *compliance* a dover essere "irrobustita"). Il consolidato orientamento

June 2021, EBA/REP/2021/17. Si veda, inoltre, D. BROEDERS, J. PRENIO, FSI INSIGHTS ON POLICY IMPLEMENTATION NO. 9: INNOVATIVE TECHNOLOGY IN FINANCIAL SUPERVISION (SUPTECH) – THE EXPERIENCE OF EARLY USERS 2–3, 17–19 (Bank for In'l Settlements 2018). Tra le letture "tradizionali", v. W. ARNER, J.N. BARBERIS, R.P. BUCKEY, *FinTech, RegTech, and the reconceptualization of financial regulation*, in *Northwestern Journal of International Law & Business*, 2016(a), 37(3), 371; D.A. ZETZSCHE, R.P. BUCKLEY, D.W. ARNER, J.N. BARBERIS, *From FinTech to TechFin: The regulatory challenges of data-driven finance*, in *New York University Journal of Law and Business*, 2017, 14, 393; D.W. ARNER, R.P. BUCKLEY, J. BARBERIS, *A FinTech and RegTech Overview: Where We Have Come from and Where We Are Going*, in Idd. (a cura di), *The RegTech Book*, Chichester, 2019; N.G. PACKIN, *Regtech, Compliance and Technology Judgement Rule*, in *Chi.-Kent L. Rev.*, 2018, Vol. 93, Issue I, 193; R.H. WEBER, *RegTech as A New Legal Challenge*, in *J. Fin. Transformation*, 2017, 46, 10. S. DI CASTRI, S. HOHL, A. KULENKAMPFF AND J. PRENIO, *The suptech generations*, FSI Insights on policy implementation, no 19, October 2019; K. BEERMAN, J. PRENIO AND R. ZAMIL, *Suptech tools for prudential supervision and their use during the pandemic*, FSI Insights on policy implementation, no 37, December 2021. Quanto alla letteratura domestica, si rimanda a M. RABITTI, A. SCIARRONE ALIBRANDI, *RegTech e SupTech*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza Artificiale e Diritto: Una Rivoluzione?*, Astrid, 2022, 451.

[47] Per un contributo "fondativo" in termini generali, R. BALDWIN, M. CAVE, M. LODGE, *Understanding Regulation. Theory, Strategy, and Practice*, Oxford, 2012, 259; in termini più sintetici, N. GUNNINGHAM, *Enforcement and Compliance Strategies*, in R. BALDWIN, M. CAVE, M. LODGE (Eds.), *The Oxford Handbook of Regulation*, Oxford, 2010, 120. Cfr., inoltre, M. PELLEGRINI, *L'intelligenza artificiale nell'organizzazione bancaria: quali sfide per il regolatore?*, in *Riv. trim. dir. econ.*, 2021, III, 422 e, spec., 438.

per una disciplina *principle-based* e *risk-based*[48], come quella del Regolamento, connotata da ampi margini di discrezionalità e di valutazione per l'Autorità di vigilanza, in una logica di *adaptive regulation*[49], sembra confermare queste perplessità.

Guardando al Regolamento, è evidente che la sua "messa a terra" si realizzerà, almeno inizialmente, con un approccio *bottom-up* (più chiaramente, "dal basso") e su impulso degli operatori finanziari[50]; ma non meno importante sarà, per raggiungere una normazione minima, ma uniforme, in materia di IA finanziaria, un intervento regolatorio a livello di mercato, che accompagni e riorienti gli sforzi di *governance* delle singole entità finanziarie. Ciò perché, come detto, le specificità del fenomeno rendono la gestione dei requisiti normativi e "di processo" stabiliti dal Regolamento, con tutti i costi di *compliance* annessi, un compito oneroso per gli intermediari finanziari e per tutte le imprese che entrano a far parte della catena del valore dell'IA finanziaria.

La complessità di queste sfide richiede una *governance* dell'IA finanziaria a più livelli, che si componga di diverse fonti di intervento, utili ad integrare i requisiti generali e l'architettura "complessiva" dell'AI Act nel settore finanziario.

E, di fatti, l'AI Act, dal punto di vista della tecnica regolatoria, contrappone al suo ambito applicativo ristretto alcuni strumenti di *soft law*, destinati a integrare la normativa di primo livello, e suscettibili di

---

[48] Cfr. G. DE GREGORIO, P. DUNN, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, 2022, 59(2), 473 ss.; M. EBERS, *Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, in *Journal of European Journal of Risk Regulation*, 2024, 1.

[49] L.G. BAXTER, *Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures*, 66 Duke L. J., 2016, 567.

[50] Un esempio per tutti è la documentazione tecnica che le entità che producono o utilizzano sistemi ad alto rischio devono fornire alle autorità di vigilanza nazionali (senza considerare che le stesse autorità possono richiedere ai fornitori di IA di dimostrare la conformità del sistema di IA ad alto rischio ai requisiti normativi stabiliti). Sebbene ne siano destinatari le autorità di vigilanza nazionali, in prima battuta, i richiamati obblighi informativi a carico delle imprese coinvolte nella catena del valore dell'IA attivano un flusso informativo destinato a confluire verso il Consiglio per l'IA. Cfr. art. 11, art. 16, par. 1, lett. j), art. 20 e art. 66, lett. a), b) e c) del Regolamento.

adattare o estendere i requisiti posti dal Regolamento secondo un approccio *bottom-up* e di "sperimentazione progressiva".

In questo contesto, il Regolamento traccia una parabola che dai principi normativi generali muove verso soluzioni di auto-regolamentazione, individuando quali strumenti rilevanti per la disciplina dei sistemi di IA standard tecnici[51], codici di condotta[52] e *sandbox regolamentari*[53].

Questi ultimi strumenti sono accomunati dalla loro dimensione istituzionale, in quanto sono approvati ed emanati (come nel caso delle norme tecniche e dei codici di condotta) o supervisionati (come nel caso delle *sandbox* di regolamentazione) dalle autorità competenti. D'altronde, tali strumenti di *soft law* condividono una funzione di co-regolazione, giacché permettono la convivenza e la compenetrazione della lettera della norma con le istanze emergenti dal mercato. E, al tempo stesso, permettono di sfruttare gli spazi "lasciati liberi" dalle "maglie strette" del Regolamento, così da incentivare soluzioni innovative e scongiurare un'applicazione eccessivamente rigida dei requisiti regolatori e penalizzante per gli attori di mercato potenzialmente "nuovi entranti" nel mercato.

Del resto, un approccio di co-regolamentazione alla *governance* dei requisiti normativi non appare nuovo nel contesto della regolamentazione finanziaria: precursore, in questo senso, è stata la c.d. "procedura Lamfalussy", considerata come uno strumento di regolamentazione efficace grazie al coinvolgimento di diverse parti interessate e in grado di calibrare le norme di principio ai rischi in concreto riscontrati e alle condizioni di mercato[54].

[51] Cfr. art. 40 del Regolamento.

[52] Cfr. art. 95 del Regolamento.

[53] Cfr. Considerando 25, 138-143, art. 57, 58, 59 del Regolamento.

[54] Sul tema, si v. D. ALFORD, *The Lamfalussy Process and EU Bank Regulation: Another Step on the Road to Pan-European Regulation?*, in *Annual review of banking & financial law*, 2006, 25, 1.

4. *Le disposizioni in tema di vigilanza inserite nel Regolamento sull'Intelligenza Artificiale*

4.1. *Vigilanza "tradizionale", vigilanza "tecnologica" e l'adeguata organizzazione interna*

Non sfugge come tutto quanto sopra riportato abbia conseguenze in punto di supervisione, dal momento che la Direttiva sui requisiti patrimoniali ("CRD IV"), all'art. 74[55], la sua trasposizione nel Testo Unico Bancario ("TUB")[56] e nelle disposizioni di vigilanza di Banca d'Italia[57] impongono che la supervisione verifichi che l'intermediario sia dotato di un'adeguata organizzazione interna[58].

Ciò evidentemente implica che le autorità di vigilanza (Banca Centrale Europea e Banca d'Italia) debbano poter verificare e "mappare" se tra i processi che la banca adotta ve ne siano alcuni gestiti, in tutto o in parte, con l'ausilio di tecnologie di IA e in che misura, quindi, ciò abbia un impatto e rientri nel perimetro di valutazione e nel

[55] Direttiva 2013/36/UE del Parlamento Europeo e del Consiglio del 26 giugno 2013 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE.

[56] In special modo, il pensiero va all'art. 67 TUB che offre la base giuridica alle conseguenti disposizioni di vigilanza.

[57] Cfr. Circolare di Banca d'Italia n. 285 del 17 dicembre 2013 – Disposizioni di vigilanza per le banche, nel suo ultimo aggiornamento n. 49 del 23 luglio 2024, e, più nello specifico, il Titolo IV "Governo societario, controlli interni, gestione dei rischi" della Parte Prima "Recepimento in Italia della CRD IV".

[58] A tal proposito, è bene ricordare che, in astratto, in mancanza di precedenti giurisprudenziali sul punto, ogni carenza organizzativa potrebbe integrare la violazione dell'art. 74 della CRD. Tale principio di diritto è stato applicato in materia di contrasto al riciclaggio dalle pronunce del Tribunale (Nona Sezione ampliata) del 6 ottobre 2021, cause riunite T-351/18 e T-584/18, Ukrselhosprom PCF e Versobank contro Banca centrale europea, ECLI:EU:T:2021:669 e della Corte di giustizia (Prima Sezione) del 7 settembre 2023, causa C-803/21, Versobank AS contro Banca centrale europea, ECLI:EU:C:2023:630. Del resto, poiché la BCE non ha competenze di vigilanza in materia di contrasto al riciclaggio, se ne potrebbe dedurre che, anche in una materia ancora in fase di definizione e, quindi, in caso di ricorso all'IA, l'intermediario potrebbe incorrere in una violazione dell'art. 74.

sindacato della vigilanza[59] senza correre il rischio di indebite "invasioni di campo" e sovrapposizioni con altre autorità, come il Garante per la protezione dei dati personali, l'Agenzia per la Cybersicureza Nazionale o l'Autorità Garante per la Concorrenza e il Mercato e senza "esorbitare" dalle finalità tradizionali dell'attività di vigilanza (garantire la sana e prudente gestione, la stabilità, l'efficienza e la competitività del sistema bancario).

4.2. *La vigilanza nella Proposta di Regolamento*

In questo scenario, "entra in gioco" e si inserisce l'AI Act, che, per la gran parte del testo, non si occupa di imprese bancarie, né di sistema finanziario ma che, ciononostante, recepisce (neanche tanto) surrettiziamente, alcuni propositi "di sistema" a dir poco deflagranti.

Andando con ordine, la Proposta di Regolamento[60] proponeva che le autorità di vigilanza finanziaria (e, quindi, anche quelle di vigilanza prudenziale) svolgessero il compito di supervisori dell'IA.

In particolare, il Considerando 80 della Proposta di Regolamento proponeva che «[…] *le autorità responsabili del controllo e dell'applicazione della normativa in materia di servizi finanziari, compresa, se del caso, la Banca centrale europea,* [fossero] *designate come autorità competenti ai fini del controllo dell'attuazione del presente regolamento, anche in relazione alle attività di vigilanza del mercato, per quanto riguarda i sistemi di IA forniti o utilizzati da istituti finanziari regolamentati e sottoposti a vigilanza*».

[59] In altri termini, nel caso un intermediario faccia ricorso a modelli interni per il calcolo dei requisiti di capitale ponderati per i rischi ("*risk weighted assets*"), l'Autorità di vigilanza dovrebbe poter verificare e, se del caso, sindacare il percorso "argomentativo" e "logico" attraverso cui si sarebbe giunti a un tale risultato, a prescindere dal fatto se tale modelli statistici interni si servano o meno di tecnologie di IA. Allo stesso modo, l'attività di ispezione effettuata presso un intermediario bancario deve poter verificare l'attività di valutazione del merito creditizio dei suoi clienti, sia che la valutazione sia condotta da una persona fisica sia che venga portata dall'IA (o con l'ausilio di quest'ultima).

[60] 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, Bruxelles, 21.4.2021, COM(2021) 206 final, 2021/0106(COD).

Non solo: la Proposta di Regolamento proponeva di modificare alcune disposizioni della CRD IV per integrare nel quadro prudenziale elementi riguardanti la valutazione di tecnologie applicate all'IA.

Più nello specifico, si intendeva integrare negli obblighi e nelle procedure esistenti a norma della CRD IV la procedura di valutazione della conformità e alcuni degli obblighi procedurali dei fornitori in materia di gestione dei rischi, monitoraggio successivo alla commercializzazione e documentazione. Ciò significa – volendo tradurre il (talvolta) criptico periodare dei testi normativi del legislatore europeo – che la gestione dei sistemi di IA, per le banche, ricade nell'ambito delle regole di *governance* interna e dell'applicazione delle procedure in materia di gestione dei rischi. Di conseguenza, non stupisce il rimando esplicito all'art. 74 della CRD IV[61] che, come visto, prevede che le banche debbano dotarsi di solidi dispositivi di governo societario, di una chiara struttura dell'organizzazione, nonché di processi efficaci per l'identificazione, la gestione, la sorveglianza e la segnalazione dei rischi ai quali esse sono o potrebbero essere esposte. La medesima impostazione è stata applicata al caso del controllo di qualità dei sistemi di IA, che rimanda ai meccanismi di *governance* delle banche di cui all'art. 74 della CRD IV[62].

A questo punto, emergono svariate perplessità interpretative.

Come noto, già dalla Proposta, si distingueva principalmente tra fornitori e *deployer*, ossia tra chi sviluppa il sistema di IA e lo immette sul mercato o in servizio sotto la propria responsabilità, e chi lo utilizza. In linea di principio, sui fornitori di sistemi IA ricadono la maggior parte degli obblighi previsti dalla Proposta (e ora dal Regolamento), e quindi dei relativi costi di *compliance*. Nell'ottica del legislatore europeo, ciò si rendeva necessario dal momento che questi operatori economici sono responsabili dello sviluppo dei sistemi di IA, considerata come la fase più sensibile nel relativo ciclo di vita e in cui è possibile predisporre e approntare misure di mitigazione per la maggior parte dei rischi insiti in un tale applicativo.

Ora, dal momento che, nella maggior parte dei casi, le banche acquistano tecnologie piuttosto che svilupparle, sorge il dubbio se il rapporto dialettico tra la Proposta di Regolamento e la CRD IV muti a

[61] Cfr. art. 9, par. 9, della Proposta di Regolamento.
[62] Cfr. art. 17, par. 3, della Proposta di Regolamento.

seconda che la banca sia *provider* o mero *deployer* di applicazioni di IA.

Ad esempio, la Proposta[63] e il successivo AI Act approvato[64] impongono ai fornitori di IA: (i) di redigere la documentazione tecnica che spieghi la tecnologia adottata, (ii) di osservare le norme per valutare la conformità della tecnologia prima della sua "immissione nel mercato", nonché (iii) di predisporre un sistema di conservazione dei *log* generati automaticamente dal sistema di IA.

Tutte queste disposizioni chiariscono poi che, qualora il fornitore sia una banca, queste tre attività debbono ricadere "sotto l'ombrello" dell'architettura di *governance* interna disegnata dall'art. 74 della CRD IV.

Ebbene, da più parti, si sono correttamente sollevati dubbi circa la praticabilità di una siffatta soluzione, dal momento che dovrebbe essere il fornitore del *software* e dell'applicativo di IA (che la banca di volta in volta utilizza) ad essere assoggettato a tali obblighi (piuttosto che la banca stessa, del resto il più delle volte estranea e non coinvolta in tali attività)[65].

L'altro "binario" di sovrapposizione tra la Proposta di Regolamento e il diritto bancario "tradizionale" (su cui è intervenuto un ripensamento all'atto della predisposizione del testo finale dell'AI Act) riguardava il regime relativo alla valutazione di conformità cui sono onerati i sistemi di IA ad altro rischio in base ai quali gli stessi debbono rispondere a precisi requisiti tecnici prima di poter essere forniti ed utilizzati[66].

Ancora una volta è il fornitore a dover dimostrare la conformità di un sistema di IA ad alto rischio, a seguito di una procedura di auto-verifica (v. allegato VI) oppure attraverso una procedura di valutazione da parte di un soggetto terzo (i.e., un organismo notificato di cui all'allegato VII).

Nel caso in cui il sistema di IA sia fornito o "messo in servizio" da una banca, la Proposta di Regolamento stabiliva che «*la valutazione della conformità* [sarebbe stata] *effettuata nell'ambito della procedura di cui agli articoli da 97 a 101* [della CRD IV]», vale a dire in base al

[63] Cfr. artt. 18, 19 e 20 della Proposta di Regolamento.

[64] Cfr. artt. 11, 17, 18, 19, 43, 46 47 del Regolamento.

[65] Si rimanda a R. LENER, *Vigilanza prudenziale e intelligenza artificiale*, in *Riv. trim. dir. econ.*, 2022, I, 214.

[66] Cfr. artt. 43 e 41 della Proposta di Regolamento.

processo di revisione e di valutazione prudenziale (*Supervisory Review and Evaluation Process*, più noto come SREP), che rappresenta una procedura portata avanti dai supervisori per valutare la situazione, non solo patrimoniale, della banca e connotato da più marcata valenza prudenziale. Ciò evidentemente avrebbe trascinato l'Autorità di vigilanza in un "terreno poco familiare", dal momento che la valutazione di conformità sarebbe stata di natura sostanzialmente diversa rispetto a quella prevista dall'AI Act: non sarebbe stata condotta, cioè, *ex ante* come richiesto dall'art. 43 della Proposta, ma solo *ex post*, in conformità alla natura della valutazione condotta dall'Autorità di vigilanza prudenziale nel contesto dello SREP[67].

4.3. *La posizione della BCE*

Dinnanzi a un tale "reticolo" di disposizioni, è comprensibile il disorientamento cui si è assistito, soprattutto proveniente da parte della Banca Centrale Europea ("BCE") in qualità di autorità di supervisione europea.

Ciò non tanto in considerazione delle "strettoie" del mandato della BCE, che, ai sensi dell'art. 127, par. 6, TFUE, limita la devoluzione delle competenze alla BCE ai compiti specifici in merito alle politiche che riguardano la vigilanza prudenziale degli enti creditizi e delle altre istituzioni finanziarie. Il rischio sarebbe stato quello di un affidamento *ultra vires* del ruolo di supervisore dell'IA[68] che avrebbe cozzato con la prudenza della BCE nell'intervenire in materia contigue e adiacenti, come dimostrato dal caso dell'anti-riciclaggio[69]. Ma, soprattutto,

[67] Cfr. *infra* Parere della Banca Centrale Europea del 29 dicembre 2021 relativo a una proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (CON/2021/40) (2022/C 115/05), par. 2.2.5.

[68] Soprattutto, tenendo conto della base giuridica dell'AI Act, vale a dire l'art. 114 TFUE.

[69] Corte di giustizia, sentenza del 22 giugno 2022, causa T-797/19, Anglo Austrian e BeleggingMaatschappij "Far-East" BV v ECB, ECLI:EU:T:2022:389. Rimanendo a questo esempio, il 19 giugno 2024 è stato pubblicato sulla Gazzetta ufficiale dell'Unione europea il Regolamento (UE) 2024/1624 del Parlamento e del Consiglio del 31 maggio 2024 relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo ("AMLR"), che entrerà in vigore il ventesimo giorno successivo alla sua pubblicazione e si applicherà a partire dal 10

perché, pur tenendo sullo sfondo il dato normativo, le Autorità di vigilanza prudenziale non sono equipaggiate per diventare, da un giorno all'altro, Autorità di vigilanza e supervisione della tecnologia, non solo dal punto di vista delle competenze.

Si è fatta strada, in altri termini, la convinzione generalizzata che la sorveglianza di un mercato come quello dell'IA non abbia natura intrinsecamente prudenziale, giacché l'obiettivo non è quello di preservare la stabilità finanziaria, ma di scongiurare l'utilizzo fraudolento delle applicazioni di IA, a scapito degli interessi dei consumatori e dei diritti individuali.

In questi termini, si esprime chiaramente la BCE nella sua Opinione sulla Proposta di Regolamento[70], secondo cui «[…] *la BCE suggerisce che, per essere coerente con le sue competenze in materia di vigilanza prudenziale ai sensi dell'articolo 127, paragrafo 6, del trattato e del regolamento sull'MVU* [il Meccanismo di Vigilanza Unico ndr], *il testo della proposta di regolamento dovrebbe chiarire in modo inequivocabile che la BCE non è designata come autorità di vigilanza del mercato né incaricata di compiti di vigilanza del mercato*»[71].

Di conseguenza, «*la BCE evince che il legislatore dell'Unione non propone che la BCE agisca come autorità di vigilanza del mercato in*

luglio 2027. Il 19 giugno 2024 è stata pubblicata anche la Direttiva (UE) 2024/1640 relativa ai meccanismi che gli Stati membri devono mettere in atto per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che abroga la Direttiva (UE) 2015/849 ("AMLD6"). In tali documenti si delinea compiti e poteri di un'apposita Authority che, tra le altre cose, avrà il compito, richiamando la CRD IV, all'art. 117, par. 5, di condividere con le autorità di vigilanza prudenziale informazioni rilevanti per i loro compiti. Si rimanda al Parere della BCE del 16 febbraio 2022 relativo a una proposta di regolamento che istituisce un'Autorità per la lotta al riciclaggio e al finanziamento del terrorismo (CON/2022/4) (2022/C 210/05). Si veda ancora E. MCCAUL, *Anti-money laundering and banking supervision*, speech at Leaders in Finance AML Europe 2023 event, Brussels, 29 June 2023.

[70] Parere della Banca Centrale Europea del 29 dicembre 2021 relativo a una proposta di regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (CON/2021/40) (2022/C 115/05).

[71] Parere della Banca Centrale Europea del 29 dicembre 2021, cit., punto 2.1.6. Si ribadisce, al punto 1.6., che si auspica un chiarimento del ruolo della BCE, specialmente per quanto riguarda: (1) le competenze di vigilanza prudenziale della BCE in generale e relativamente alla vigilanza del mercato e alla valutazione della conformità, e (2) l'applicazione della Proposta rispetto all'assolvimento dei compiti della BCE ai sensi del TFUE.

relazione agli enti creditizi sottoposti alla sua vigilanza ai sensi della proposta di regolamento. Tale conclusione è in linea con i considerando del regolamento sull'MVU, i quali chiariscono che le autorità nazionali sono competenti a garantire un livello elevato di tutela dei consumatori»[72].

In modo ancor più cristallino, la BCE si pronuncia in favore di un approccio neutrale dal punto di vista tecnologico nella vigilanza prudenziale degli enti creditizi[73], proponendosi di mantenere condizioni di parità, all'insegna del principio-guida e del mantra del «*same activity, same risks, same rules*»[74].

Il parere della BCE esprime, dunque, una posizione ragionevole e costituisce un crocevia ineludibile nel contesto "dinamico" della vigilanza bancaria e dell'IA.

Non si auspica solo una definizione più chiara del ruolo della BCE ai fini della vigilanza sull'IA "finanziaria". Ma si propone che la vigilanza sulle tecnologie debba "incarnare" il modello della vigilanza "per attività" in luogo di quella "per soggetti", proprio in ragione della trasversalità delle applicazioni di IA che possono servire ad una banca per profilare un cliente, oppure ad una piattaforma di *social network* per offrire una pubblicità "su misura" agli utenti. Ciò non deve arrivare al punto di privare l'Autorità di vigilanza degli strumenti per verificare eventuali elementi di rischio per il governo societario, la stabilità patrimoniale e, in generale, l'attività della banca. Del resto, si tratta di predisporre un flusso informativo minimo e un'impalcatura di

[72] Parere della Banca Centrale Europea del 29 dicembre 2021, cit., punto 2.1.5.

[73] Scendendo sul piano della pratica, può aiutare un esempio: se la banca utilizza sistemi di IA per valutare il merito di credito di un cliente, la BCE potrà valutare siffatta tecnologia sotto il profilo della sana e prudente gestione, ma non sotto il profilo della tutela del consumatore/utente cui venga erogato o rifiutato il finanziamento richiesto e che eventualmente potrà rivolgersi all'Autorità garante della Concorrenza e del Mercato o al Garante privacy (ma non certo all'autorità di supervisione) in caso di doglianze che coinvolgano profili consumeristici o *privacy*.

[74] Si rimanda a quanto riportato da Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), *30 Recommendations on Regulation, Innovation and Finance* (Dec 2019); European Commission, A Digital Finance Strategy for the EU (Sep 2020); Financial Stability Board, Global Regulatory Framework for Crypto-asset Activities (17 July 2023). Cfr. la relazione di A. ENRIA (Presidente del Consiglio di vigilanza della BCE), *A binary future? How digitalisation may change banking*, De Nederlandsche Bank, Amsterdam, 11 marzo 2019, disponibile sul sito Internet della vigilanza bancaria della BCE.

supervisione prudenziale già inclusa nell'art. 74 della CRD IV, là dove si richiede che la banca si doti di un solido sistema di *governance*.

4.3. *La "chiusura del cerchio" nel testo finale del Regolamento: il livello "nazionale"*

Scendendo sempre più nello specifico – e guardando dentro le "maglie" del testo finale Regolamento nel suo rapporto con la regolazione di settore –, il coordinamento tra vigilanza dell'IA e la vigilanza finanziaria rimane un tassello prioritario nel più complesso mosaico dell'architettura istituzionale dell'IA[75].

In primo luogo, l'art. 70 del Regolamento impone agli Stati membri di designare una o più autorità nazionali competenti, con funzioni di vigilanza del mercato e della sua corretta applicazione[76]. Gli Stati membri possono decidere se creare un'autorità di controllo per l'IA *ad*

[75] Si veda, per alcuni primi commenti, G. SCHNEIDER, *La proposta di regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)*, in *Resp. civ. prev.*, 2023, III, 1014 ss.; S. PELLERITI, *Breve analisi della* governance *istituzionale delineata nella proposta di regolamento UE sull'Intelligenza Artificiale*, in *Riv. trim. dir. econ.*, 2021, Suppl. III, 280; S. VILLANI, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sè?,* in *Quaderni AISDUE*, 2024, I, 1.

[76] Secondo il paragrafo 3 della medesima disposizione, è necessario che le Autorità nazionali competenti «*dispongano di sufficiente personale permanentemente disponibile, le cui competenze e conoscenze comprendono una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di IA, della protezione dei dati personali, della cibersicurezza, dei diritti fondamentali, dei rischi per la salute e la sicurezza e una conoscenza delle norme e dei requisiti giuridici esistenti*». Gli Stati membri possono decidere di nominare qualsiasi tipo di soggetto pubblico, conformemente alle loro specifiche caratteristiche ed esigenze organizzative nazionali. Tuttavia, il paragrafo 1 ricorda che le autorità dovranno agire «*in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti nell'applicazione e attuazione del regolamento*». Il rinvio a tali requisiti è benvenuto e in linea con i compiti affidati alle autorità che, pur non essendo organi giurisdizionali, avranno anche poteri investigativi e correttivi. In argomento, v. L. TORCHIA, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista trimestrale di diritto pubblico*, 2022, IV, 1110.

hoc[77] o affidare le relative funzioni e responsabilità ad un'autorità indipendente già esistente[78].

Si tratta essenzialmente di un'attività di supporto dal momento che le autorità potranno fornire orientamenti e consulenza sull'attuazione del Regolamento, in particolare in favore delle PMI, comprese le *start-up*. Ma non solo. Si prefigura, poi, la vera e proprio funzione di vigilanza. Sebbene, infatti, la maggior parte dei sistemi di IA non sia soggetta a requisiti e obblighi specifici in quanto non categorizzati come ad alto rischio, le Autorità di vigilanza del mercato potranno adottare misure in relazione a tutti i sistemi di IA che presentino un rischio conforme al Regolamento[79], chiedendo ai fornitori informazioni, accedendo alla documentazione, sollecitando l'adozione di misure correttive e il ritiro del sistema di IA dal mercato, se necessario[80]. Com'è ovvio, l'esercizio da parte dell'Autorità di

[77] L'AI Act articola i poteri delle Autorità di vigilanza create *ex novo* rinviando esplicitamente al sistema istituito dal Regolamento (UE) 2019/1020 sulla vigilanza del mercato e la conformità dei prodotti.

[78] In Italia, il confronto si è rivelato particolarmente serrato: il governo ha affidato, infatti, i compiti di vigilanza all'Agenzia per l'Italia Digitale e all'Agenzia per la Cybersicurezza. Dall'altra, il Garante Privacy ha rivendicato il proprio ruolo privilegiato nell'attuazione dell'AI Act, «*in ragione della sua competenza sulle norme da applicare e delle sue caratteristiche di indipendenza*. […] *Il Garante possiede infatti, già oggi, i requisiti di competenza e, assieme, indipendenza necessari per garantire un'attuazione del Regolamento coerente con l'obiettivo di garanzia di un livello elevato di tutela dei diritti fondamentali nel ricorso all'IA, sancito dall'art. 1, p. 1*». Si rimanda, per approfondimenti, al Garante per la protezione dei dati personali, Segnalazione al Parlamento e al Governo sull'Autorità per l'Intelligenza Artificiale del 25 marzo 2024.

[79] Artt. 79-80 del Regolamento.

[80] Fatti salvi i poteri di controllo di propria iniziativa, ai sensi dell'art. 73, l'adozione delle menzionate misure potrebbe avvenire a seguito della ricezione di segnalazioni relative a gravi incidenti da parte dei fornitori di IA, di cui l'Autorità di vigilanza dovrà informare gli organismi pubblici nazionali nonché la Commissione sulla base di quanto già previsto dagli artt. 19 e 20 del Regolamento (UE) 2019/102010. Oppure, come stabilito dall'art. 85, «*qualsiasi persona fisica o giuridica*» che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni dell'AI Act potrà presentare all'Autorità di vigilanza un reclamo motivato. Qualora le misure correttive di cui sopra non siano sufficienti, l'art. 99 introduce la possibilità per le Autorità di vigilanza di adottare sanzioni pecuniarie e altre misure di esecuzione, inclusi avvertimenti e misure di natura non pecuniaria, applicabili in caso di violazione del Regolamento da parte degli operatori.

vigilanza del mercato dei poteri sanzionatori dovrà essere soggetto alle garanzie procedurali previste dal diritto dell'Unione e da quello nazionale, incluso il diritto ad un ricorso giurisdizionale effettivo[81].

In secondo luogo, per i sistemi di IA ad alto rischio immessi sul mercato, messi in servizio o usati da istituti finanziari disciplinati dal diritto dell'Unione in materia di servizi finanziari, l'autorità di vigilanza del mercato (una nozione, questa, che necessiterà di ulteriori affinamenti) è l'autorità nazionale responsabile della vigilanza finanziaria di tali enti, nella misura in cui l'immissione sul mercato, la messa in servizio o l'uso del sistema di IA siano direttamente collegati alla fornitura di tali servizi finanziari[82].

Dunque, in linea con l'autonomia procedurale degli Stati membri, la dimensione organizzativa delle Autorità di vigilanza (e anche la distribuzione dei poteri rispetto all'imposizione di eventuali sanzioni in caso di violazioni dell'AI Act) è demandata alle normative nazionali.

Tuttavia, il Regolamento prevede tre eccezioni. La prima è indicata all'art. 74, par. 3, secondo cui, salvo diversa e motivata decisione adottata a livello nazionale, l'Autorità di vigilanza del mercato per i sistemi collegati a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A (vale a dire, la normativa relativa ai prodotti già sottoposti a controlli nel quadro del mercato interno), sarà quella già designata a norma di tali atti giuridici. In secondo luogo, stando all'art. 74, par. 6 del Regolamento, per i sistemi di IA ad alto rischio immessi sul mercato, messi in servizio o usati da istituti finanziari disciplinati dal diritto dell'Unione in materia di servizi finanziari e creditizi, l'autorità di vigilanza del mercato sarà quella responsabile della vigilanza finanziaria (art. 74, par. 6). La terza eccezione, prevista all'art. 74, par. 8, riguarda i sistemi utilizzati a fini di attività di contrasto, gestione delle

[81] Cfr. art. 99, par. 10, AI Act. È verosimile immaginare che i provvedimenti adottati dalle Autorità di vigilanza possano essere sottoposti al sindacato delle Corti nazionali (e, nel caso, della Corte di giustizia tramite un rinvio pregiudiziale) nel rispetto, nuovamente, dell'art. 47 della Carta dei diritti fondamentali dell'Unione Europea.

[82] Cfr., art. 74, par. 3, AI Act. In questo senso, è prevista anche una deroga, in ragione della quale, tenuta ferma l'esigenza e la garanzia di coordinamento, lo Stato membro può individuare un'altra autorità competente come autorità di vigilanza del mercato ai fini dell'operatività del Regolamento.

frontiere, giustizia e tutela dei processi democratici nonché i sistemi di IA ad alto rischio elencati nell'allegato III[83]: in questi casi, gli Stati membri dovranno designare come Autorità di vigilanza del mercato le autorità di controllo competenti per la protezione dei dati a norma del Regolamento (UE) 2016/679 ("GDPR") e della Direttiva (UE) 2016/680 (c.d. "Direttiva Polizia")[84].

Le riserve di competenza espressamente previste dall'AI Act sono finalizzate ad evitare che le attività di vigilanza pregiudichino la capacità delle autorità già esistenti di svolgere i loro compiti secondo quanto previsto dal diritto dell'Unione.

Dai potenziali conflitti di attribuzione del potere di vigilanza a diverse autorità discenderà l'esigenza di rintracciare un punto di equilibrio e un coordinamento tra queste per garantire la "messa a terra" del Regolamento a livello degli Stati membri. Un problema di *governance* "istituzionale", quest'ultimo, già affrontato dalla Corte di giustizia nel 2023 nel caso Meta Platforms e al[85] e dal Consiglio di Stato nel caso Telepass c. AGCM[86]. Nel caso riguardante Meta, si lamentava il fatto che il ricorso, da parte delle Autorità garanti della concorrenza alle disposizioni del GDPR per contestare una condotta in ipotesi anti-competitiva (o, comunque, rilevante ai fini del diritto della concorrenza) avrebbe determinato una potenziale lesione delle competenze dei Garanti privacy. La Corte di giustizia ha riconosciuto alle autorità amministrative degli Stati membri la possibilità di esercitare una competenza condivisa, purché non sostitutiva, facendo

[83] Nel dettaglio, la disposizione fa riferimento all'utilizzo dei sistemi di IA per la raccolta di dati biometrici (Allegato III, punto 1) e ai sistemi ad alto rischio previsti nell'Allegato III, punti 6, 7 e 8. Da notare che le autorità per la protezione dei dati dovrebbero auspicabilmente presentare alla Commissione una relazione annuale sull'uso dei sistemi di identificazione biometrica "in tempo reale"; un auspicio che, tuttavia, è contemplato esclusivamente nel Considerando 36 ma non si rinviene nel testo del Regolamento.

[84] Si fa riferimento alla Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[85] Corte di giustizia, sentenza 4 luglio 2023, causa C-252/21, sentenza Meta Platforms Inc and Others v Bundeskartellamt, ECLI:EU:C:2023:537.

[86] Consiglio di Stato, Sez. VI, 15 gennaio 2024, n. 497.

discendere direttamente dal principio di leale collaborazione, previsto dall'art. 4, par. 3, TUE un dovere di collaborazione e di coordinamento tra dette autorità.

Calando l'argomentazione della Corte di giustizia al caso dell'AI Act, parrebbe verosimile sostenere che, se questo ragionamento "tiene" per Autorità di vigilanza con competenze istituzionali e *mission* differenti ma che si allineano nella pratica, *a fortiori* ciò vale per le autorità amministrative espressamente titolate ad intervenire per vigilare sull'attuazione dell'IA, che dovranno cooperare tra loro al fine di garantire, da un lato, l'effettiva applicazione della normativa di settore e, dall'altro, la coerenza del sistema di protezione istituito dal Regolamento[87]. Questa urgenza è pure desumibile dalla risalente giurisprudenza della Corte di giustizia, secondo cui le autorità amministrative degli Stati membri debbono assistersi reciprocamente nell'adempimento dei compiti derivanti dai Trattati, adottare ogni misura necessaria per assicurare l'adempimento degli obblighi risultanti dagli atti adottati dalle istituzioni, nonché evitare di adottare qualsiasi misura che potrebbe compromettere il raggiungimento degli obiettivi dell'Unione[88].

Da ultimo, l'importanza della leale collaborazione è emersa pure nel corso del G7 privacy tenutosi a Roma[89] e sta affiorando sempre più anche nella letteratura scientifica[90].

Ad ogni modo, è giocoforza attendersi nel breve-medio termine un intervento della Corte di giustizia che chiarisca questo aspetto controverso e non disciplinato dal Regolamento; ciò per scongiurare il rischio di interpretazioni divergenti tra le diverse Autorità di vigilanza

[87] M. KLAMERT, *Article 4 TEU*, in M. KELLERBAUER (eds.), *The EU Treaties and the Charter of Fundamental Rights – A Commentary*, Oxford, 2019, 35; F. CASOLARI, *La leale cooperazione tra Stati membri e Unione europea. Studio sulla partecipazione all'Unione al tempo delle crisi*, Napoli, 2020, *passim*.

[88] Corte di giustizia, sentenza 7 novembre 2013, causa C-518/11, UPC Nederland, punto 59; Corte di giustizia, sentenza 1 agosto 2022, cause C-14/21 e C-15/21, Sea Watch, punto 156.

[89] Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI, 11 ottobre 2024, par. 16.

[90] Da ultimo, P. DE HERT, P. HAJDUK, *EU cross-regime enforcement, redundancy and interdependence. Addressing overlap of enforcement structures in the digital sphere after Meta*, in *Technology & Regulation*, 2024, I, 291.

nazionali circa l'attività di supervisione sull'attuazione del Regolamento.

4.4. *Il livello sovra-nazionale: il ruolo della BCE*

Si disegna (verrebbe da dire, si abbozza) anche un tentativo di coordinamento "istituzionale" sovra-nazionale e intersettoriale, dal momento che le Autorità nazionali di vigilanza del mercato che controllano gli enti creditizi (quelle che rientrano nel quadro della CRD IV) sono chiamate a comunicare alla BCE qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per i compiti in materia di vigilanza prudenziale[91].

Il punto di caduta di questo disegno "istituzionale" si rinviene nell'art. 74 e nei Considerando 155-158 del Regolamento ed è pienamente in linea con le indicazioni della BCE nel contesto del suo parere sull'originaria Proposta di Regolamento.

Più nello specifico, per quanto riguarda i servizi finanziari basati sull'IA, la BCE manterrà le sue funzioni di vigilanza prudenziale sui processi di gestione del rischio e sui meccanismi di controllo interno

[91] Più nello specifico, secondo il Considerando 158, «[a]*l fine di garantire la coerenza dell'applicazione e dell'esecuzione degli obblighi previsti* […] *in materia di servizi finanziari, è opportuno che le autorità competenti del controllo e dell'esecuzione di tali atti giuridici, in particolare le autorità competenti qual definite al regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio e alle direttive 2008/48/CE, 2009/138/CE, 2013/36/UE, 2014/17/UE e (UE) 2016/97 del Parlamento europeo e del Consiglio, siano designate, nell'ambito delle rispettive competenze, quali autorità competenti ai fini del controllo dell'attuazione del presente regolamento, anche in relazione alle attività di vigilanza del mercato, per quanto riguarda i sistemi di IA forniti o utilizzati da istituti finanziari regolamentati e sottoposti a vigilanza, a meno che gli Stati membri non decidano di designare un'altra autorità per svolgere tali compiti di vigilanza del mercato.* […] *È opportuno prevedere che, quando agiscono in qualità di Autorità di vigilanza del mercato a norma del presente regolamento, le Autorità nazionali responsabili della vigilanza degli enti creditizi disciplinati nel quadro della direttiva 2013/36/UE, che partecipano al meccanismo di vigilanza unico istituito dal regolamento (UE) n. 1024/2013 del Consiglio, comunichino senza ritardo alla Banca centrale europea qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per i compiti in materia di vigilanza prudenziale della Banca centrale europea specificati in tale regolamento*».

degli enti creditizi[92]. Tali processi e meccanismi possono riguardare anche le soluzioni tecnologiche adottate dagli enti creditizi e rientrano nei poteri di vigilanza prudenziale della BCE solo nella misura in cui tali soluzioni possano avere un impatto sulla sicurezza e sulla solidità degli enti creditizi e sulla stabilità del sistema finanziario[93].

Tale competenza "funzionale" della BCE sui sistemi di IA è ormai parte del bagaglio acquisito dei cultori del diritto dell'economia, giacché la Corte di giustizia, in casi più o meno recenti (basti pensare, solo per citarne alcuni, ai casi *ESMA Short Selling*[94], FBF[95], Corneli[96] e tenendo sullo sfondo i "pilastri" Meroni[97] e Romano[98]), ha posto l'accento sull'importanza dei "plasmare" i poteri di natura discrezionale delle Autorità di vigilanza finanziarie nello svolgimento dei compiti di regolazione e supervisione degli intermediari bancari[99], soprattutto in

[92] Parere della Banca Centrale Europea del 29 dicembre 2021, cit., punto 2.3.

[93] *Ivi*, par. 2.1.4.

[94] Corte di giustizia, sentenza del 22 gennaio 2014, Regno Unito c. Parlamento e Consiglio, Causa C-270/12, par. 53.

[95] Corte di giustizia (Grande Sezione), sentenza del 15 luglio 2021, Fédération bancaire française (FBF) c. Autorité de contrôle prudentiel et de résolution, Causa C-911/19, ECLI:EU:C:2021:599.

[96] Corte di giustizia, sentenza del 12 ottobre 2022, Francesca Corneli c. Banca Centrale Europea, Causa T-502/19, ECLI:EU:T:2022:627.

[97] Corte di giustizia, sentenza del 13 giugno 1958, Meroni & Co., Industrie Metallurgiche, società in accomandita semplice contro l'Alta Autorità della Comunità europea del Carbone e dell'Acciaio, C-10-56, 69 ss., ECLI:EU:C:1958:8.

[98] Corte di giustizia, sentenza del 14 maggio 1981, Giuseppe Romano c. Institut National D'Assurance, C-98/80.

[99] Si vedano, per un inquadramento di ordine generale sul tema (a prescindere dai singoli casi trattati), i contributi di M. CHAMON, *EU Agencies between "Meroni" and "Romano" or the Devil and the Deep Blue Sea*, in *Common Market Law Review*, 2011, 48, 1057; F. ANNUNZIATA, *The Remains of the Day: EU Financial Agencies, Soft Law and the Relics of Meroni*, EBI Working Paper Series 2021 n. 106, 19 November 2021, 27-29; F. ANNUNZIATA, T. BRAGA DE ARRUDA, *The Corneli Case and the Application of National Law by the European Central Bank*, Bocconi Legal Studies Research Paper No. 4477503, 22 June 2023; A. WITTE, *The Application of National Banking Supervision Law by the ECB: Three Parallel Modes of Executing EU Law?* in *Maastricht Journal of European and Comparative Law*, 2014, Vol. 21, Issue I, 89; L. BOUCON, D. JAROS, *The application of national law by the European Central Bank within the EU Banking Union's Single Supervisory Mechanism: A new mode of European integration?*, in *European Journal of Legal Studies*, 2018, X, 155. Per un ottimo contributo recente che ripercorre tutte le tappe appena tratteggiate, si

coincidenza temporale con la realizzazione del Meccanismo di vigilanza unico (MVU)[100].

rimanda a D. VESE, A Game of Thrones*: ruolo e poteri dell'autorità bancaria europea alla luce degli orientamenti della Corte di Giustizia*, in questa *Rivista*, 2023, I, 1.

[100] Per un'impostazione teorica sul MVU, si v. F. CAPRIGLIONE, *L'Unione bancaria. Una sfida per un'Europa più unita*, Torino, 2013, *passim*, che chiarisce come tale meccanismo segni un'importante tappa nel processo di integrazione europea tramite un progetto tecnico che mira a rafforzare la costruzione dell'UE. Per ulteriori approfondimenti, si v. S. ANTONIAZZI, *Il meccanismo di vigilanza prudenziale. Quadro d'insieme*, in M.P. CHITI, V. SANTORO (a cura di), *L'Unione bancaria europea*, Pisa, 2016, 175. Inoltre, si v. E. FERRAN, V.S.G. BABIS, *The European Single Supervisory Mechanism*, in *Journal of Corporate Law Studies*, 2013, 13, II, 255. Solo per riannodare i fili della discussione, si ricorderà, sino ad epoca recente – e anche sulla scorta dei lavori preparatori del Regolamento MVU (e poi SSM), – l'opinione prevalente era nel senso di escludere che alla BCE spettassero poteri di natura regolamentare nel contesto della vigilanza prudenziale, essendo questi ultimi attribuiti all'EBA, e non alla BCE (e ciò al fine di non violare il principio di conferimento delle competenze). Come noto, il MVU è stato creato con il Regolamento (UE) n. 1024/2013 del Consiglio del 15 ottobre 2013 che attribuisce alla Banca centrale europea compiti specifici in merito alle politiche in materia di vigilanza prudenziale degli enti creditizi. Il Regolamento (UE) n. 468/2014 della Banca centrale europea del 16 aprile 2014 (noto come "regolamento quadro sull'SSM") ha istituito il quadro di cooperazione nell'ambito del MVU tra la Banca centrale europea e le autorità nazionali di vigilanza. Il MUV, operativo dal 1 novembre 2014, è uno dei pilastri fondamentali dell'Unione bancaria europea. L'apparentemente granitico fronte dottrinale ha cominciato, tuttavia, ad incrinarsi non soltanto in quanto autorevoli interpreti hanno messo in discussione la bontà della scelta operata, ma anche perché, più di recente, la conclusione in precedenza raggiunta è stata oggetto di ripensamenti. Il *vulnus* alla teoria della insussistenza in capo alla BCE di poteri di natura regolamentare è venuto a crearsi in relazione all'esercizio delle discrezionalità che la normativa europea di primo livello lascia alle Autorità nazionali competenti. Più nello specifico, come noto, nel corso degli anni si è assistito a una tensione, ancora perdurante, fra il processo di "accentramento" che ha interessato soprattutto la *governance* bancaria a seguito degli eventi innescati dalla crisi del 2008 con il conferimento di una posizione di preminenza agli organi centrali dell'UE, oltre che di più penetranti poteri amministrativi accordati alla BCE rispetto al passato e la sussistenza di elementi di ampio decentramento amministrativo, con il rilevante ruolo svolto dalle autorità nazionali nell'ambito della *governance* bancaria multilivello, disegnata dal legislatore europeo successivamente alla crisi finanziaria del 2008. Il tema dell'attribuzione alla BCE di compiti di natura regolamentare ha rappresentato un punto focale della nuova architettura della vigilanza: v., in proposito, già E. WYMEERSCH, *The European Banking Union, a first analysis*, *Financial Law Institute*, Working Paper, 2012-7, 4. Per un inquadramento di quei poteri, che vengono

Fermo quanto precede, il peso crescente che la BCE ha acquisito nel panorama complessivo della vigilanza – e che viene a rafforzarsi come conseguenza dell'AI Act – pone il problema dello svolgimento di funzioni regolamentari da parte della BCE ben al di là dei limiti sopra tracciati, e, segnatamente, per il tramite di strumenti di "*soft law*". Interpretazioni, linee guida, orientamenti, pareri, prassi di vigilanza – tutti campi sui quali la BCE è fortemente impegnata – finiscono, infatti, per avere un impatto tanto maggiore quanto più è "autorevole" la fonte dalla quale promanano.

In un modello che tende ad assumere una configurazione sempre più verticistica, nel quale si amplia, di fatto, il peso della BCE, il rilievo della *soft law* che promana da quest'ultima è, dunque, inevitabilmente destinato ad aumentare, e il Regolamento fornisce, naturalmente, notevole supporto a questa tendenza. Il fenomeno, peraltro, si accentuerà nel tempo, man mano che la stessa BCE stratificherà *expertise*, prassi di vigilanza, orientamenti, pareri, linee-guida. Esso tenderà ad annacquare la (tendenziale) rigida ripartizione di ruoli tra regolamentazione e vigilanza che ispira l'architettura del sistema di vigilanza europeo, e porrà sempre di più sul campo il tema, di non agevole soluzione, dei rapporti tra BCE e EBA[101].

Seguendo questa "pista", al di fuori di tali compiti di vigilanza prudenziale, la BCE non dovrebbe essere titolare di alcuna competenza per i compiti di vigilanza del mercato evidenziati *supra* nei Considerando 155-158. Ciononostante, già il parere della BCE "lasciava una porta aperta", non escludendo l'attribuzione di poteri di

esercitati nel contesto della formulazione degli ITS e RTS, E. FERRAN, *The Existential Search of the European Banking Authority*, ECGI Law Working Paper, n. 297/2015; S. DEL GATTO, *Il problema dei rapporti tra la Banca Centrale Europea e l'Autorità Bancaria Europea*, in *Riv. trim. dir. pubb.*, 2015, IV, 1243. Più di recente, si rimanda a A. WITTE, K. LACKHOFF, "Art. 4 SSMR" in Brussels Commentary on the European Banking Union (eds. J. Binder, C. Gortsos, K. Lackhoff, and C. Ohler), Baden-Baden: Beck C. H., 2022, 71; A. BROZZETTI, *La vigilanza nell'ambito del Meccanismo di vigilanza unico,* in A. NIGRO (a cura di), *Giurisprudenza bancaria (2016-2017)*, Milano, 2019, 64.

[101] Si rimanda a M. ORTINO, *Le competenze regolatorie dell'Unione europea in materia bancaria*, Torino, 2021, *passim*; ID., *Il* soft law *nella disciplina dei mercati finanziari*, in *Banca impr. soc.*, 2020, I, 93; F. ANNUNZIATA, M. LAMANDINI, "*Questo è un nodo avviluppato": divagazioni sulla regolazione del mercato finanziario?*, in *Giur. comm.*, 2022, I, 34.

sorveglianza del mercato in materia di sistemi di IA alle autorità nazionali competenti designate per la vigilanza degli enti creditizi, per ragioni di coerenza e di efficacia dei risultati di vigilanza in termini di costi[102]. E in questo senso si deve leggere, infatti, l'aggiunta relativa alla necessità, da parte delle Autorità nazionali di vigilanza del mercato ai sensi della CRD IV, di riferire alla BCE qualsiasi informazione individuata nel corso delle loro attività di vigilanza del mercato, che possa essere di potenziale interesse per la vigilanza prudenziale della stessa BCE.

4.5. *Il livello sovra-nazionale: il ruolo dell'AI Office e del Consiglio per l'IA*

A dimostrazione delle frizioni e dei rischi di sovrapposizione, il Regolamento prevede che, per i sistemi di IA impiegati dalle istituzioni dell'Unione, l'autorità competente ai fini di vigilanza sia il Garante europeo della protezione dei dati ("EDPS"). In questo caso, tuttavia, la BCE ha sottolineato l'importanza di limitare la vigilanza delle autorità europee e nazionali di protezione dei dati sui sistemi di IA eventualmente adottati dalla BCE o dalle banche centrali nazionali, in modo da preservare l'indipendenza delle autorità finanziarie nello svolgimento dei compiti a queste conferiti dal TFUE[103]. Un'altra invasione di campo, forse, o, quantomeno, lo sconfinamento verso la

[102] Cfr. Parere della Banca Centrale Europea del 29 dicembre 2021, cit., par. 2.2.3.

[103] Si legge, al par. 2.4. della Parere della Banca Centrale Europea del 29 dicembre 2021, cit., che «[è] *importante sottolineare che la BCE e le BCN* [le Banche centrali nazionali, n.d.r.] *dovrebbero essere in grado di svolgere in modo indipendente i compiti ad esse attribuiti dal trattato, ad esempio quando utilizzano qualsiasi applicazione di intelligenza artificiale per definire e attuare la politica monetaria e per promuovere il regolare funzionamento dei sistemi di pagamento. Occorre tuttavia riconoscere che l'indipendenza del SEBC* [Sistema europeo di banche centrali, n.d.r.] *nello svolgimento dei suoi compiti non lo esonera da ogni norma di diritto dell'Unione. La BCE evince che qualsiasi eventuale vigilanza della BCE da parte del GEPD* [Garante europeo della protezione dei dati, n.d.r.] *e delle BCN da parte delle autorità nazionali competenti sarebbe limitata a controlli adeguati su un sistema di IA e sulla* governance *del sistema stesso e non sarebbe in alcun modo intesa a pregiudicare la capacità della BCE e delle BCN di svolgere in modo indipendente i compiti loro attribuiti dal Trattato*».

consacrazione del principio della competenza funzionale, che va, però, meglio calibrato e "centellinato".

Un ulteriore livello di complicazione scaturisce dall'analisi del perimetro della governance dell'IA nell'Unione, che ha ricadute decisive in punto di supervisione e nel cui contesto si distinguono quattro attori principali: il Consiglio europeo per l'intelligenza artificiale (European Artificial Intelligence Board, o anche Consiglio per l'IA)[104], l'AI Office[105], il Forum consultivo e il Gruppo scientifico di esperti indipendenti[106].

In linea di principio, il Consiglio per l'IA dovrebbe coordinare la cooperazione tra le autorità di vigilanza nazionali e la Commissione nel campo della regolamentazione dell'IA, promuovere l'analisi delle questioni emergenti e l'individuazione di *best practices* nel campo dell'IA. In altri termini, tale organo dovrebbe rivestire una funzione consultiva, estendendo le sue competenze alla Commissione e agli Stati membri e favorendo un processo decisionale informato nel campo dell'IA. Il Forum consultivo e il Gruppo scientifico di esperti indipendenti rappresentano, invece, organismi di esperti indipendenti, designati a fornire approfondimenti tecnici al Consiglio per l'IA e alla Commissione, così idealmente rafforzando le basi dello sviluppo e della regolamentazione dell'IA. A ciò si aggiungono, come detto, un livello di *governance* anche a livello nazionale, in cui ogni Stato membro è tenuto a nominare autorità nazionali competenti per la notifica e la vigilanza dei sistemi di IA, che operino in autonomia, imparzialità e indipendenza (anche a livello di risorse).

Al contempo, la Commissione istituirà apposite strutture di prova e di supporto alla sperimentazione dell'IA per assistere le attività di sorveglianza del mercato e di conformità[107], confermando l'importanza dell'ambiente controllato delle *sandbox* di regolamentazione ai fini di sviluppo, sperimentazione e la convalida di sistemi innovativi di IA.

A tal proposito, sono proprio le *sandbox* regolatorie il "terreno di elezione" in cui si sviluppano le prime forme di collaborazione tra Autorità di vigilanza nazionali e Consiglio per l'IA, alle quali quest'ultimo è chiamato a partecipare insieme alle autorità nazionali

[104] Cfr. art. 65 del Regolamento.
[105] Cfr. art. 64 del Regolamento.
[106] Cfr. Considerando 151 del Regolamento.
[107] Cfr. art. 84 e Considerando 152 del Regolamento.

competenti (che rimangono i *dominus* rispetto ai poteri di poteri di vigilanza e correttivi delle autorità che supervisionano la *sandbox*)[108], sempre con l'obiettivo di adattare al nuovo Regolamento eventuali sperimentazioni di applicazioni *Fintech*, che, anche qui, dovrebbero essere improntate al principio «*stessa attività, stesso rischio, stesse regole*»[109].

Di là dal caso delle *sandbox*, l'AI Act promuove uno sforzo di cooperazione "ad ampio spettro" del Comitato, anche, se del caso, con gli organismi, i gruppi di esperti e le reti dell'UE pertinenti, in particolare nei settori dei servizi finanziari e delle criptovalute[110], che dovrà confluire nell'emanazione di linee guida, pareri e raccomandazioni (anche unitamente alle autorità nazionali competenti nel settore finanziario)[111] e che contribuiranno a definire il quadro "dinamico" dell'IA all'interno della regolamentazione finanziaria di settore.

Inoltre, una banca dati comune dell'Unione raccoglierà informazioni sui sistemi di IA ad alto rischio, che dovranno essere registrati dai fornitori e dai *deployer* prima dell'immissione sul mercato o dell'utilizzo[112]. I *deployer* dovranno, poi, istituire sistemi di monitoraggio post-vendita per i sistemi di IA ad alto rischio e rispettare i requisiti e i divieti stabiliti dal Regolamento[113]. Gli Stati membri dovranno stabilire regole per le sanzioni in caso di non conformità, che potranno arrivare fino a 35 milioni di euro o al 7% del fatturato mondiale annuo per le pratiche di IA vietate[114]. Gli obblighi di riservatezza si applicheranno, poi, a tutti gli attori coinvolti nell'applicazione del Regolamento, rispettando i diritti di proprietà intellettuale e i segreti commerciali[115].

Un discorso a parte va fatto in relazione all'AI Office, istituito lo scorso gennaio 2024 all'interno della Commissione[116] con lo scopo di

[108] Cfr. art. 57, par. 15, 16, 17 del Regolamento.
[109] Cfr. art. 58 del Regolamento.
[110] Cfr. art. 66, lett. h) del Regolamento.
[111] Cfr. art. 66, lett. e) del Regolamento.
[112] Cfr. artt. 49, par. 1, 71 e Considerando 131 del Regolamento.
[113] Cfr. art. 72, par. 1 e 2 e Considerando 155 del Regolamento.
[114] Artt. 99, par. 3 e 101, par. 1 del Regolamento.
[115] Artt. 53, par. 1, lett. b) e 78, par. 1, insieme ai Considerando 3 e 88.
[116] Decisione della Commissione del 24 gennaio 2024 che istituisce l'Ufficio europeo per l'intelligenza artificiale (C/2024/1459), Art. 1.

garantire lo sviluppo e il coordinamento della politica sull'AI a livello europeo, oltre che di supervisionare l'attuazione e l'applicazione del Regolamento[117]. L'assunto è che tale neo-costituito Ufficio debba lavorare in continuità e a strettissimo contatto con il Consiglio per l'IA, ma i rischi di tale doppio binario sono, a tutt'oggi, ancora inesplorati[118].

Più nello specifico, il mandato dell'AI Office consiste nel contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e dei modelli di IA per finalità generali (modelli GPAI)[119], compresa l'adesione ai codici di condotta approvati[120] e unitamente al supporto alla *governance* dell'IA[121]. Attraverso una rigorosa supervisione delle misure di applicazione, l'AI Office ha l'autorità di richiedere informazioni e documentazione ai fornitori di modelli di AI per scopi generali, di condurre valutazioni complete dei loro sistemi[122], e di imporre misure per garantire la conformità o attenuare i rischi[123]. L'AI Office garantisce, inoltre, l'esercizio di taluni diritti procedurali agli operatori economici di modelli di AI per scopi generali, consentendo loro di contestare potenziali violazioni del Regolamento.

Sebbene il suo mandato principale possa essere identificato nel garantire conformità al Regolamento[124], si possono rinvenire cinque principali gruppi di competenze dell'AI Office[125]:

a. In primo luogo, è stato affidato un ruolo di vigilanza e di *enforcement*, in base al quale l'AI Office ha l'autorità di avviare "dialoghi strutturati", vale a dire scambi sistematici di informazioni,

[117] Cfr. art. 64 del Regolamento.

[118] Cfr., come esempio, l'art. 66, lett. k) del Regolamento, che, in maniera estremamente vaga, impone al Consiglio per l'IA di «*assistere l'Ufficio per l'IA nel sostenere le autorità nazionali competenti nell'istituzione e nello sviluppo di spazi di sperimentazione normativa per l'IA e facilitare la cooperazione e la condivisione di informazioni tra gli spazi di sperimentazione normativa per l'IA*».

[119] Cfr. Considerando 97 del Regolamento.

[120] Considerando 117 del Regolamento.

[121] Art. 3, par. 47, del Regolamento.

[122] Art. 92, par. 1 e Considerando 164 del Regolamento.

[123] Art. 93 e Considerando 164 del Regolamento.

[124] Considerando 148 del Regolamento.

[125] Per un'analisi completa del ruolo dell'AI Office, si rimanda a M.L. PASSADOR, *AI in the Vault: AI Act's Impact on Financial Regulation*, in corso di pubblicazione in *Loyola University of Chicago Law Review*, 2025; ID., *AI Act and the ECB: Steering Financial Supervision in the EU*, in corso di pubblicazione in *Columbia Journal of European Law*, 2025, Volume 30, II.

dati e approfondimenti tra gli organismi di regolamentazione e i *provider* di modelli GPAI[126], assicurando trasparenza, responsabilità e aderenza agli standard normativi, di richiedere a questi ultimi informazioni e documentazione in merito ai *test* interni, e alle procedure di contenimento del rischio[127], di condurre valutazioni complete dei loro sistemi, in particolare per quanto riguarda i rischi sistemici[128], e di attuare misure per garantire la conformità o l'attenuazione dei rischi.

A ben vedere, i poteri dell'AI Office sono di duplice natura. Da un lato – a dimostrazione del suo ruolo "proattivo" –, l'AI Office è autorizzato a richiedere e ottenere la documentazione tecnica dei modelli GPAI[129], le copie dei mandati dei rappresentanti autorizzati dei *provider*[130] e, più in generale, «*su richiesta motivata* [...] *tutte le informazioni e la documentazione per dimostrare il rispetto degli obblighi*»[131]. D'altro canto, in senso opposto, l'AI Office sarà il destinatario di tutte informazioni in virtù degli obblighi imposti ai fornitori di modelli GPAI, che dovranno notificare allo stesso Ufficio quando si viene a conoscenza del fatto che un modello GPAI soddisfa (o soddisferà in futuro) i requisiti che presentano un rischio sistemico[132], mentre il rappresentante autorizzato dovrà revocare il proprio mandato e informare l'AI Office se il fornitore violi il Regolamento[133]. Inoltre, l'AI Office sarà destinatario di un flusso informativo proveniente anche da altri enti pubblici, come le relazioni annuali sulle *sandbox* regolamentari delle Autorità nazionali[134].

b. In secondo luogo, l'AI Office svolge un ruolo centrale nella prevenzione dell'uso improprio dei sistemi di IA. In questa veste, dovrebbe promuovere lo sviluppo di codici di condotta, linee guida volontarie volte a garantire un'IA etica e affidabile a livello europeo. A tal fine, l'AI Office deve collaborare con le Autorità nazionali competenti, consultarsi con le organizzazioni della società civile, con

[126] Cfr. art. 91, par. 2 del Regolamento.
[127] Cfr. art. 88 del Regolamento.
[128] Cfr. art. 92, par. 1 e par. 7 del Regolamento.
[129] Art. 53, par. 1 del Regolamento.
[130] Cfr. art. 54, par. 2 del Regolamento.
[131] Art. 54, par. 3, lett. c) del Regolamento.
[132] Considerando 112 del Regolamento.
[133] Art. 53, par. 5 del Regolamento.
[134] Art. 57, par. 9, lett. b) e par. 15 del Regolamento.

gli esperti e con altri organismi che si occupano di IA, come il Gruppo di esperti scientifici[135]. Inoltre, deve facilitare la stesura di codici di condotta per l'applicazione volontaria di requisiti specifici a tutti i sistemi di IA, che rappresentano un'altra forma di auto-regolamentazione per i *provider* di IA[136]. A dimostrazione di ciò, la Commissione si riserva il diritto di autorizzare e validare un codice di condotta scelto e un codice di buon pratiche, se ritenuto opportuno dall'AI Office[137]. In aggiunta a quanto sopra, l'AI Office dovrebbe promuovere la convergenza delle migliori pratiche nelle procedure di appalto pubblico nel settore, che sono le procedure attraverso le quali le autorità pubbliche acquistano i sistemi di IA[138].

c. In terzo luogo, l'AI Office fungerà da "cardine" attorno a cui convergeranno le Autorità nazionali, gli altri organismi europei che si occupano di IA, i fornitori e gli utilizzatori. In particolare, fornirà informazioni alle autorità nazionali su richiesta e, se del caso, per accertare la non conformità dei sistemi di IA ad alto rischio[139]. Inoltre, svolgerà un ruolo di supporto nei confronti del Consiglio per l'IA, partecipando, senza diritto di voto, alle riunioni di quest'ultimo, facilitandone i lavori e contribuendo alla predisposizione dell'ordine del giorno[140]. Da ultimo, aggiornerà attivamente il Consiglio per l'IA su eventuali allarmi relativi a rischi sistemici e sulle misure attuate in risposta (in genere, i *follow-up* tradizionali riguarderanno principalmente le indagini)[141].

Queste situazioni di allarme saranno segnalate dal Gruppo scientifico di esperti indipendenti, che è parzialmente supervisionato dall'AI Office, in quanto responsabile della definizione di procedure per prevenire (e gestire) i conflitti di interesse all'interno del Gruppo di esperti[142]. Inoltre, il Gruppo di esperti indipendenti svolgerà un ruolo cruciale per l'AI Office, fornendo a quest'ultimo organismo consulenza

[135] Art. 56 e Considerando 116 del Regolamento.
[136] Art. 75, par. 2 e art. 95, par. 1 del Regolamento.
[137] Considerando 117 del Regolamento.
[138] Art. 62, par. 3, lett. d) del Regolamento.
[139] Art. 75, par. 3 del Regolamento.
[140] Art. 65, par. 2 e par. 4 del Regolamento.
[141] Art. 90, par. 2 e Considerando 163 del Regolamento.
[142] Art. 68, par. 4 del Regolamento.

a livello generale e sostenendo le sue attività di monitoraggio[143]. L'AI Office può anche offrire assistenza per il coordinamento delle indagini congiunte condotte dalle Autorità nazionali di vigilanza del mercato, incaricate di sorvegliare e far rispettare la conformità dei sistemi di AI ad alto rischio[144]. Infine, l'AI Office assisterà e consiglierà le Autorità nazionali nella creazione di *sandbox* regolamentari[145].

d. In quarto luogo, il nuovo Ufficio ha il compito di svolgere una serie di attività rivolte al pubblico, come, ad esempio, coordinare campagne di comunicazione volte a sensibilizzare il settore sugli obblighi derivanti dal Regolamento[146], creare una piattaforma unica per la diffusione delle informazioni[147] e pubblicare un registro delle *sandbox*[148]. Inoltre, è responsabile della fornitura di modelli e *template* per la sintesi dei dati di utilizzati per l'attività di *training* dei modelli GPAI[149] e, su richiesta del Consiglio dell'IA, di altri eventuali *template* utili allo scopo[150]. Ancora, l'AI Office può predisporre e proporre termini contrattuali-modello da utilizzare su base volontaria dai fornitori di sistemi di IA ad alto rischio e da terze parti che forniscono strumenti, servizi, componenti o processi utilizzati nei sistemi di IA ad alto rischio[151].

5. *Una ricostruzione critica del "reticolo" di competenze nella supervisione dell'IA (e alcune proposte di riforma)*

Il *focus* del presente contributo si è appuntato principalmente sullo scenario istituzionale e sulla struttura di *governance* del Regolamento, ma, nel prossimo futuro, è verosimile che si presentino ulteriori sfide riguardanti l'interazione tra l'AI Act e le altre normative nazionali e internazionali di interesse per il governo dell'IA. A livello

[143] Art. 68, par. 3 e Considerando 163 del Regolamento.
[144] Art. 75, par. 2 e Considerando 161 del Regolamento.
[145] Art. 57, par. 15 del Regolamento.
[146] Art. 62, par. 3, lett. c) del Regolamento.
[147] Art. 62, par. 3, lett. b) del Regolamento.
[148] Art. 57, par. 16 del Regolamento.
[149] Art. 53, par. 1, lett. d) del Regolamento.
[150] Art. 62, par. 3, lett. a) del Regolamento.
[151] Art. 25, par. 4 e Considerando 90 del Regolamento.

A livello europeo, sarà urgente valutare e "testare" nuove forme di coordinamento, in particolare alla luce delle potenziali sovrapposizioni con il GDPR[152], il *Digital Markets Act* ("DMA")[153] e il *Digital Services Act* ("DSA")[154].

A livello internazionale, la necessità di allineamento è altrettanto pressante e non meno controversa, tenuto conto dell'approccio all'argomento dei due maggiori attori politici globali, la Cina[155] e gli Stati Uniti[156].

---

[152] Un esempio emblematico in questo senso è la limitazione provvisoria del trattamento, ai sensi dell'art. 58, par. 2, lett. f) del GDPR disposta nel marzo 2023 dal Garante privacy italiano, nei confronti di Open AI, società statunitense sviluppatrice del prodotto "ChatGPT", definibile, ai sensi dell'AI Act, come GPAI. Con un comunicato stampa del 29 gennaio 2024 il Garante Privacy rendeva noto di aver notificato a OpenAI l'atto di contestazione per aver violato, sotto molteplici profili, la normativa in materia di protezione dei dati personali. Più di recente, con provvedimento n. 755 del 2 novembre 2024 [doc. web n. 10085455], il Garante ha adottato un provvedimento correttivo e sanzionatorio con cui ha comminato ad OpenAI una sanzione di 15 milioni di euro e ingiunto la realizzazione di una campagna informativa di sei mesi. Tale decisione muove dall'*interim report* prodotto a maggio 2024 dalla *task force* istituita dall'EDPB. Cfr. Report of the work undertaken by the ChatGPT Taskforce, 23 maggio 2024. Si veda ancora E. DROUARD, O. KUROCHKINA, R. SCHLICH, D. OZTURK, *The Interplay between the AI Act and the GDPR: Part II – Compliance Challenges for AI Systems That Use Personal Data*, in *AIRe*, 2024, III, 297 ss. Per una guida sulle principali sfide della Generative AI alla privacy, cfr. EDPS, Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems, 3 giugno 2024.

[153] Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), L 265/1, 12.10.2022.

[154] Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), L 277/1, 27.10.2022.

[155] La Cina ha emanato diverse normative mirate in tema di IA, comprese quelle che riguardano esplicitamente l'IA generativa. Cfr. S. MIGLIORINI, *China's Interim Measures on generative AI: Origin, content and significance*, in *Computer Law and Security Review*, Volume 53, 2024, 105985.

[156] Negli Stati Uniti manca attualmente un modello di *governance* dell'IA, in quanto il quadro giuridico esistente (l'*executive order* del Presidente, Joe Biden) ha un campo di applicazione e meccanismi di attuazione limitati. Norme divergenti a

In un contesto siffatto, è ovvio che il Regolamento è un "cantiere aperto" e, ciononostante, diverse proposte di modifica possono essere avanzate e divenire oggetto di discussione pubblica[157].

In prima battuta, occorrerà riconoscere ancor più centralità e delineare ancor più nitidamente il ruolo dell'AI Office. Del resto, è già stato riconosciuto che, a valle dell'entrata in vigore del Regolamento, ben potranno essere apportate modifiche significative alla sua operatività, al fine di migliorarne la sua capacità di adempiere agli obblighi e facilitare la supervisione dell'Unione su specifiche tecnologie di IA. A tal proposito, sarà richiesto alla Commissione di presentare al Parlamento e al Consiglio dell'UE una valutazione sull'operato dell'AI Office, verificando se i poteri e le competenze conferiti siano adeguati rispetto agli obiettivi del Regolamento[158].

Più nello specifico, sarebbe auspicabile una maggiore chiarezza sui termini dell'indipendenza operativa dell'AI Office. Sarebbero altrettanto utili delle linee guida che ne delineino il mandato decisionale, l'indipendenza finanziaria e le capacità di coinvolgimento di soggetti esterni[159].

---

livello statale (come la legge sull'IA della California SB 1047, su cui di recente il governatore della California, Gavin Newsom ha posto il veto) potrebbero creare un mosaico problematico anche all'interno degli Stati Uniti, rendendo ancora più difficile l'allineamento con l'AI Act. Cfr. M WÖRSDÖRFER, *Biden's Executive Order on AI and the E.U.'s AI Act: A Comparative Computer-Ethical Analysis, in Philosophy & Technology*, 2024, 37, 74.

[157] Si veda, per un dettagliato dibattito sul tema, C. NOVELLI, P. HACKER, J. MORLEY, J. TRONDAL, L. FLORIDI, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities,* in *European Journal of Risk Regulation*, 2024, 1 ss.

[158] Cfr. Art. 112 del Regolamento.

[159] Secondo C. NOVELLI, P. HACKER, J. MORLEY, J. TRONDAL, L. FLORIDI, *op.cit.*, 20 ss., un approccio alternativo, potenzialmente più efficace, consisterebbe nell'organizzazione dell'AI Office come agenzia decentrata dotata di personalità giuridica, alla stregua dell'European Food Safety Authority (EFSA) e dell'European Medicines Afenct (EMA). Il decentramento, concepito per i settori cardine del mercato unico, conferirebbe all'AI Office una maggiore autonomia, tra cui una relativa libertà dalle agende politiche a livello di Commissione, una missione definita, poteri esecutivi e l'autorità di emettere decisioni vincolanti, anche se con possibilità di appello e di review giudiziaria. Tale organizzazione aumenterebbe probabilmente l'indipendenza dell'AI Office dalla Commissione e dalla più ampia matrice istituzionale dell'Unione, posizionandolo come attore chiave nella *governance*

In secondo luogo, occorrerà razionalizzare e sistematizzare la cooperazione tra le autorità nazionali di controllo interessate a livello statale e tra queste e il Consiglio per l'IA e l'AI Office, incaricati, come visto, a vario titolo, di un'attività di *oversight* sulla corretta applicazione del Regolamento nei vari Stati membri e di elaborare linee guida in materia, specialmente in relazione ai modelli GPAI[160].

Quanto previsto dal Regolamento è senza dubbio un incoraggiante punto di partenza.

L'art. 74, par. 11 prevede, infatti, che le Autorità di vigilanza del mercato degli Stati membri e la Commissione propongano attività congiunte al fine di promuovere la conformità, sensibilizzare e fornire orientamenti in relazione all'AI Act riguardo a specifiche categorie di sistemi di IA ad alto rischio che presentino un rischio grave in due o più Stati membri. Queste attività di natura congiunta dovrebbero basarsi sulla procedura prevista all'art. 9 del Regolamento (UE) 2019/1020 sulla vigilanza del mercato e conformità dei prodotti (anche detto "Regolamento sulla sicurezza dei prodotti")[161] e sotto il coordinamento dell'AI Office.

Oltre che a raccordarsi sui codici di buone pratiche, il Regolamento prevede anche la possibilità di attivare indagini congiunte tra Autorità di vigilanza. Ai sensi dell'art. 79 par. 3, del Regolamento, se l'autorità di vigilanza di uno Stato membro ritiene che la violazione non sia limitata al suo territorio nazionale ma possa avere un impatto transnazionale, dovrà informare la Commissione e gli altri Stati membri

dell'IA. Quanto al rischio di "*agencification*", una formula usata per descrivere la possibilità di concedere agli organismi di regolamentazione un'autonomia eccessiva ma non completa, cfr. M. SCHOLTEN, M. VAN RIJSBERGEN, *The Limits of Agencification in the European Union*, in *German Law Journal*, 2014, XV, 1223; M. CHAMON, *Setting the Scene: EU Agencies, Agencification, and the EU Administration*, in M. CHAMON (ed), *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration*, Oxford University Press, 2016.

[160] Si v., su questo, anche S. VILLANI, *op.cit.*, 14.

[161] Rubricato "Attività congiunte per promuovere la conformità", secondo cui, al par. 1, «[l]*e autorità di vigilanza del mercato possono stipulare accordi con altre autorità interessate, organizzazioni che rappresentano gli operatori economici o gli utilizzatori finali per la realizzazione di attività congiunte volte a promuovere la conformità, identificando i casi di non conformità, sensibilizzando sulla normativa di armonizzazione dell'Unione e fornendo orientamenti in merito e per quanto riguarda categorie specifiche di prodotti, in particolare le categorie di prodotti che spesso presentano un rischio grave, compresi i prodotti offerti per la vendita* online».

dei risultati della valutazione e delle azioni richieste al fornitore o al *deployer* del sistema di IA. In tali casi, dovrebbe, dunque, applicarsi analogicamente la procedura relativa all'assistenza reciproca e allo scambio di informazioni nei casi transfrontalieri di cui agli artt. 22, 23 e 24 dello stesso Regolamento sulla sicurezza dei prodotti.

Inoltre, il Regolamento contempla la possibilità che qualsiasi autorità di vigilanza del mercato possa chiedere assistenza all'AI Office qualora non sia in grado di concludere un'indagine su un sistema ad alto rischio (ad esempio, a causa dell'impossibilità di accedere a determinate informazioni specifiche relative al modello GPAI su cui è costruito il sistema di IA sottoposto ad indagine[162].

Rilevante è, infine, l'art. 81 che conferma il ruolo predominante della Commissione all'interno dell'architettura complessiva del Regolamento, attribuendole una serie di poteri il cui "punto di caduta" è un criterio di prevalenza sulle decisioni delle Autorità nazionali. Infatti, è qui previsto che, qualora l'autorità di vigilanza del mercato di uno Stato membro sollevi obiezioni contro una misura adottata da un'altra autorità di vigilanza del mercato, o la Commissione ritenga che la misura sia contraria al diritto dell'Unione, quest'ultima consulterà l'Autorità di vigilanza interessata e l'operatore, e valuterà se la misura nazionale è giustificata e proporzionata. Nel caso in la Commissione la ritenga ingiustificata, la soluzione finale consisterà nel ritiro della misura nazionale da parte dello Stato membro interessato, con contestuale informativa alla Commissione.

È certamente apprezzabile lo sforzo di garantire il coordinamento e l'allineamento tra le Autorità nazionali di vigilanza, specialmente nel caso in cui si ritenga che si possa verificare un utilizzo improprio dei sistemi di IA con impatto (non solo) a livello nazionale ma anche sovranazionale. Ciononostante, tale proposito, raggiunto tramite il rinvio mobile al più generale Regolamento sulla sicurezza dei prodotti, tradisce i limiti di un siffatto meccanismo di vigilanza, costruito sì su un'impalcatura idealmente sovranazionale ma, nell'operatività, "piegato" sulle esigenze nazionali di controllo[163]. Motivo per cui è

[162] Art. 75, par. 3 del Regolamento.

[163] A conferma del carattere "programmatico" delle disposizioni di vigilanza, si rimanda alle valutazioni di S. VILLANI, *op.cit.*, 16, secondo cui, nell'iniziale Proposta di Regolamento, il Consiglio dell'IA «*doveva essere composto dalle autorità*

particolarmente preoccupante l'impossibilità da parte del Consiglio per l'IA di sottoporre a scrutinio le decisioni prese dalle Autorità nazionali. L'assenza di qualsiasi forma di "giustiziabilità", a differenza di quanto accade per il Comitato europeo per la protezione dei dati (European Data Protection Board, EDPB) nell'ambito del GDPR, rappresenta in prospettiva una grave lacuna nell'ottica di garantire un'applicazione coerente dell'IA all'interno dell'Unione e, di nuovo, potrebbe plausibilmente condurre a interpretazioni e applicazioni divergenti del Regolamento[164].

A fronte di ciò, è il caso di interrogarsi sul rischio che le Autorità degli Stati membri possano rivendicare parallelamente la competenza in taluni casi, determinando una frammentazione dell'applicazione e, se del caso, l'adozione di decisioni contrastanti, pregiudicando, in ultima istanza, i destinatari di indagini e sanzioni amministrative. Sarà, pertanto, necessario che l'attività di *enforcement* delle autorità muova, di nuovo, dal principio di leale collaborazione previsto dall'art. 4, par. 3, TUE, attingendo ai requisiti e alle modalità di cooperazione tra

nazionali di vigilanza, compreso evidentemente il Garante europeo: in altre parole, in quanto autorità di sintesi delle singole autorità di vigilanza, il [Consiglio per l'IA] *si sarebbe auto promosso ad autorità indipendente europea. Tuttavia, questo impianto è stato mitigato a seguito dell'accordo raggiunto nel trilogo, attribuendo la funzione di* trait-d'union *rispetto alla cooperazione amministrativa al sottogruppo permanente per la vigilanza del mercato (ADCO)* [uno dei due sottogruppi permanenti per fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e notificare le autorità su questioni connesse, ndr.]*, sotto il coordinamento della Commissione che mantiene ben saldo il potere regolatorio. Resta da chiedersi fino a che punto il* [Consiglio]*, che potrà sostanzialmente adottare solo atti di* soft law*, potrà garantire una supervisione (seppur debole) sull'applicazione uniforme del regolamento. Ciò, tenuto poi conto che il Garante europeo parteciperà al Comitato solamente in qualità di osservatore, smorzando così il carattere sovranazionale del coordinamento*».

[164] Su questa falsariga C. NOVELLI, P. HACKER, J. MORLEY, J. TRONDAL, L. FLORIDI, *op.cit.*, 22 ss. hanno proposto di consolidare il Forum consultivo e il Gruppo scientifico di esperti indipendenti in un soggetto giuridico unico che combinerebbe l'ampio coinvolgimento del Forum consultivo con le competenze specializzate e indipendenti del gruppo di esperti scientifici e che, insieme, potrebbero rendere un miglior servizio di supporto e consulenza al Consiglio per l'IA, all'AI Office e ad altre istituzioni o agenzie dell'Unione.

Autorità nazionali già sedimentati nella giurisprudenza della Corte di giustizia[165].

6. *Conclusioni*

In questo scritto, analizzando le disposizioni di vigilanza dell'AI Act e ponendole in relazione dialettica con la vigilanza "tradizionale", si è tentato di "accendere un faro" su alcune questioni aperte, suggerendo la necessità di un ripensamento del sistema di vigilanza dell'IA, ben oltre le soluzioni che il Regolamento e il DORA hanno appena cominciato a tratteggiare.

In chiave istituzionale e di *governance*, la direzione che è stata impressa risulta fortemente orientata a tutelare, tanto sul piano organizzativo quanto funzionale, le esigenze di controllo sull'IA degli Stati membri. Questo è confermato, in particolare, dal tenore delle disposizioni sulle Autorità di vigilanza nazionali che garantiscono ampia discrezionalità agli Stati membri nella designazione di dette autorità di vigilanza e di controllo. Solo l'AI Office si candida a presentarsi agli operatori come soggetto "terzo" che garantisca un coordinamento effettivo e stringente tra le Autorità di vigilanza, ma evidenti sono i suoi limiti strutturali. Se la BCE continuerà ad occuparsi prevalentemente di vigilanza prudenziale (interessandosi di IA, solo nei limiti in cui possa mettere a rischio la stabilità finanziaria), si conferma, in ultima istanza, l'eccessivo affidamento sull'*enforcement* delle Autorità nazionali degli Stati membri, foriero di divergenze applicative nei diversi ordinamenti.

---

[165] Corte di giustizia, sentenza 15 giugno 2021, Causa C-645/19, Facebook Ireland Limited e a. contro Gegevensbeschermingsautoriteit, ECLI:EU:C:2021:483. In quella sede, la Corte di giustizia ha confermato la ripartizione delle competenze tra le autorità di vigilanza di diversi Stati membri per preservare il cd. "*one-stop shop mechanism*" (o anche principio dello "Sportello Unico"), sottolineando l'importanza di una cooperazione non solo efficace (come espressamente previsto dall'art. 60 GDPR e dalla legislazione in materia di tutela dei dati personali) ma anche ispirata alla leale collaborazione tra di loro. Parallelamente, si fa strada nella letteratura l'applicazione del criterio di "buona amministrazione" che può fungere da principio guida e limite esterno per orientarsi nel complesso rapporto tra IA e vigilanza (anche bancaria). Si rimanda su questo al contributo di A. AZZUTTI, P.M. BATISTA, W.G. RINGE, *Good Administration in AI-Enhanced Banking Supervision: A Risk-Based Approach*, in *Columbia Journal of European Law*, 2024, Vol. 29, III, 434.

Al cuore rimane la necessità di promuovere, anche per l'IA, un'architettura di vigilanza consapevole, affidabile, trasparente e responsabile e, da qui, confermare il primato di un approccio incentrato sull'uomo e sui diritti (in linea con i valori e le norme dell'Unione, tra cui la Carta dei diritti fondamentali e la Dichiarazione europea sui diritti e i principi digitali), sia per progettazione e per impostazione predefinita nello sviluppo dei prodotti e sistemi sia per le politiche di vigilanza e supervisione[166].

[166] Si rimanda a T. EVAS, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI*, in *AIRe*, 2024, II, 89 e A. MANTALERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *Computer Law & Security Review*, 2024, 54, 106020.