DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

La governance del rischio AI nell'opinion di EIOPA: quali passi avanti?

Ottobre 2025

Giulio Giacomo Cimini, D'Argenio Polizzi e Associati

Giulio Giacomo Cimini, D'Argenio Polizzi e Associati

1. Premessa

In piena estate EIOPA, l'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali, si è risolta ad affrontare in maniera sistematica le implicazioni derivanti dall'adozione dell'intelligenza artificiale nel settore assicurativo.

Il 6 agosto 2025 è stato, infatti, pubblicato un *Impact Assessment* – una valutazione di impatto – la cui funzione principale risulta quella di valutare l'opportunità e le rispettive alternative metodologiche, di un intervento in tema di *governance* e gestione dei rischi derivanti dall'IA[1].

Il documento, sulla base della percezione che la risposta al dubbio dovesse essere affermativa, è stato pubblicato congiuntamente ad una *Opinion* – uno strumento di *soft law* paragonabile a delle linee guida – che, come si vedrà nel prosieguo, intenderebbe delineare un quadro di principi volti a guidare gli operatori nell'impiego dei sistemi di intelligenza artificiale. Principi che tengano insieme le normative settoriali e siano, al contempo, conformi ai valori fondamentali dell'ordinamento europeo[2]. L'intervento si inserisce in un contesto normativo già attraversato dal denso e sempre più popolato dibattito sul nuovo Regolamento UE in tema di intelligenza artificiale, il cd. AI Act.

Se, da una parte, l'attivismo para-regolamentare conferma la centralità del tema nell'agenda delle Autorità di vigilanza, dall'altra sembrerebbe ribadire che, sebbene la gestazione del pacchetto legislativo dell'AI Act sia stata velocizzata il più possibile per evitare che il Vecchio Continente arrancasse, il terreno di gioco rimanga, in buona sostanza, ancora caratterizzato dalle regole che furono.

Le risposte ai quesiti di *due diligence* erano e sembrerebbero ancora, per larga parte, da ricercare nelle regole classiche e già conosciute. Di qui l'intervento di EIOPA che pare aver preso le mosse da questa

1 EIOPA, 'Impact Assessment of Opinion on AI governance and risk management' (6 August 2025), consultabile al link https://www.eiopa.europa.eu/document/download/bdd11c63-5f48-442f-8291-598557af44a2_en?filename=Impact%20Assessment%20-%20Opinion%20on%20Artificial%20Intelligence%20governance%20and%20risk%20management.pdf.

2 EIOPA, 'Opinion on AI Governance and Risk Management' (6 August 2025), consultabile al link https://www.eiopa.europa.eu/document/download/88342342-a17f-4f88-842f-bf62c93012d6_en?filename=Opinion%20on%20Artificial%20Intelligence%20governance%20and%20risk%20management.pdf.

consapevolezza, ponendosi come obiettivo un riordino, per così dire, giustinianeo delle varie aspettative.

2. Il contesto nel quale si muove EIOPA (l'AI Act)

Questa decisione da parte di EIOPA, si diceva, va letta nel contesto del pacchetto di riforma che, a livello unionale, ha inaugurato l'AI Act, ovvero il Regolamento (UE) 2024/1689, pubblicato nella Gazzetta ufficiale dell'Unione Europea il 12 luglio 2024 ed entrato in vigore il 2 agosto 2024.

È utile ricordare brevemente, per mera completezza ed inquadramento sistematico, che l'AI Act, lungi dall'imporre regole di dettaglio, ha adottato un approccio cd. *risk-based*, identificando e dando priorità ai rischi più elevati ai fini della *compliance*. Un approccio regolamentare e normativo conforme allo spirito post-crisi che ha ispirato le principali altre normative del settore assicurativo[3].

L'AI Act opera, in particolare, per quel che qui può interessare, una classificazione piramidale degli strumenti di IA in quattro categorie di rischio.

Alla base della piramide figurano i sistemi a rischio minimo, come ad esempio i filtri *antispam* od i sistemi di raccomandazione, che restano al momento non regolamentati e rispetto ai quali non sussistono obblighi pregnanti per l'operatore che se ne avvalga.

In secondo luogo, risalendo l'ideale piramide, si trovano i sistemi a rischio limitato, ovvero, in ambito assicurativo, gli assistenti virtuali utilizzati per l'*onboarding* e per la preventivazione, per la distribuzione delle polizze o per la gestione dei sinistri[4]. Per questi la parola d'ordine del nuovo Regolamento UE è la trasparenza nei confronti del cliente.

Al terzo gradino si trovano i cosiddetti sistemi ad alto rischio. Tali sono, ad esempio, i dispositivi medici, o, più genericamente, quelli relativi all'accesso all'istruzione ed all'applicazione della legge. Per questi il Regolamento richiede un elevato grado di controllo imponendo un obbligo, per così dire, di rendicontazione[5]. Per rendicontazione si intende, qui, il dovere in capo alle imprese di assicurazione di registrare i set di dati, definire la necessaria supervisione umana e chiarire gli aspetti di sicurezza informatica.

I sistemi con specifici rischi di trasparenza dovranno essere segnalati come tali. In altre parole, le persone dovranno essere informate quando stanno interagendo con una macchina (*e.g.*, un *chatbot*), sono soggette a rilevamenti biometrici o stanno consumando contenuti in ogni modo generati dall'IA.

In ultimo luogo, in cima alla piramide, indicata spesso con colore rosso nelle tabelle esplicative delle Autorità, figurano i sistemi a rischio inaccettabile. Questi sono al momento vietati del tutto ed includono sistemi di polizia predittiva, di cd. *social scoring* o, più in generale, i sistemi di riconoscimento delle emozioni, nonché quelli che conferiscono piena libertà di raccomandazione algoritmica nell'utilizzo, ad esempio, dei *social network*[6].

Per quel che riguarda le imprese assicurative, il Regolamento UE prevede che queste debbano conformarsi alle nuove disposizioni entro il 2 agosto 2026. Tale lasso di tempo concerne, tuttavia, solo coloro che si avvalgano di sistemi di IA ad alto rischio cd. *standalone*[7].

Sono state previste, d'altro canto, tempistiche molto più ravvicinate, *i.e.*, il 2 febbraio 2025, per i sistemi di intelligenza artificiale proibiti ovvero dannosi o contrari ai diritti fondamentali, ed il 2 agosto 2025 per quanto, invece, attiene alla *governance* complessiva ed alle sanzioni derivanti dal mancato rispetto delle nuove disposizioni.

Per queste ultime EIOPA ha ritenuto di intervenire con l'*Opinion* di cui ci si occupa in questa sede. Tra le prime, invece, possono rientrare quelle pratiche che, facendo leva sulla forte conoscenza che l'assicuratore può avere delle abitudini dell'assicurato, abbiano come effetto ultimo una personalizzazione manipolativa delle polizze attraverso, ad esempio una categorizzazione biometrica, e finiscano con

3 Si vedano, a mero titolo esemplificativo, le disposizioni dell'art. 41 della Direttiva Solvency II, dell'art. 25 della Direttiva IDD e, più di recente, degli artt. 4,5 e 6 del Regolamento DORA.

4 Si veda l'art. 50 dell'AI Act.

5 Tra questi non rientra al momento il sistema di messaggistica ChatGPT che tante preoccupazioni ha destato ed i cui effetti dirompenti cominciano ad essere di giorno in giorno meglio valutati. Si veda in tal senso https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

6 Si veda l'art. 5 dell'AI Act.

7 Le disposizioni relative ai sistemi ad alto rischio integrati entreranno invece in vigore il 2 agosto 2027. Si vedano gli artt. 111 e 113 dell'AI Act.

il costruire dei *cluster* di rischio sulla base di attributi sensibili (*e.g.*, abitudini sessuali, appartenenza etnica o religiosa).

Dal 2 agosto 2026, si diceva, saranno, invece, applicabili le disposizioni relative ai sistemi di IA reputati di alto rischio. Tali possono essere, ad esempio, quelli che determinino l'ammontare dei premi per le polizze vita e salute[8].

Posto quanto sopra, l'impressione – di allora così come di oggi – rimane quella di essere dinnanzi ad un intervento legislativo denso di principi e *standard* la cui implementazione, essendo l'AI Act caratterizzato da una concezione orizzontale di gestione del rischio connesso, dunque cross-settoriale, non possa che poggiare sulle medesime basi normative già esistenti e note, diverse per ciascuna industria. Una circostanza che non aiuta a fugare il dubbio di un pacchetto di riforma che, pur nella sua lodevole attenzione all'uomo, abbia mancato di coraggio o, quanto meno, di specificità.

L'operatore di mercato rimane, infatti, sempre al cospetto dell'arcano sulle regole di comportamento da adottare. Un arcano dai tratti potenzialmente drammatici, se si considera che l'AI Act prevede, per i casi di *non-compliance*, sanzioni amministrative pecuniarie ben superiori a quelle tipicamente presenti, ad esempio, nel settore della gestione dei dati personali. Queste possono, infatti, raggiungere, la soglia di € 35 milioni o del 7% del fatturato globale dell'impresa, da indentificarsi non solo nel fatturato prodotto all'interno dell'Unione Europea[9].

Posto che sarà necessario un adeguamento sempre più specifico e tutto lascerebbe intendere che la strada per la vera regolamentazione settoriale in ambito assicurativo, anche alla luce dell'intervento di EIOPA, debba ancora essere battuta[10], molti si sono chiesti se, nell'attesa, sia davvero indispensabile abbandonarsi all'iperfetazione legislativa di domani o se, invece, le regole esistenti diano già indicazioni e risposte sul come comportarsi.

EIOPA, come si vedrà nel prosieguo, sembra aver accolto questa seconda e più ragionevole opzione, cominciando a tracciare qualche solco, malgrado mesi fa avesse espresso una preferenza per un sistema di regole specifiche piuttosto che cross-settoriali; regole che non impongano una *compliance* non strettamente necessaria e dunque capaci, al tempo stesso, di garantire il rispetto del principio di proporzionalità[11].

Risulta, in effetti, difficile non notare come il panorama assicurativo sia già strettamente vigilato e regolamentato da normative prudenziali sia di settore che cross-settoriali che coprono l'ambito delle decisioni automatizzate. Molta della normativa che, peraltro, interessa l'operatore assicurativo, ed in genere attivo nel più ampio settore del *bancassurance*, può definirsi come *technology-neutral*, ovvero capace di gestire, senza storture interpretative, anche i fenomeni tecnologici non previsti o prevedibili al momento della sua redazione[12].

3. L'*Impact Assessment* di EIOPA e la scelta di una *Policy* di Vigilanza

Ciò che EIOPA, conformemente alle proprie prerogative, ha inteso, *in primis*, assicurare con l'*Impact Assessment* è un'analisi costi-benefici dell'opportunità di rivolgersi alle Autorità di Vigilanza degli Stati Membri con una *Opinion* per assicurare una maggiore convergenza nella supervisione dei soggetti re-

8 Si veda l'espressa previsione contenuta all'articolo 6, co. 2, dell'AI Act e nell'Allegato III, par. 5 lett. c). Si tratta di un inserimento avvenuto dopo alterne vicende e cambi di rotta nella redazione. Ad oggi i sistemi di pricing e valutazione dei rischi, nel comparto vita e delle polizze sanitarie, sono qualificati come sistemi ad alto rischio.

9 Si veda l'art. 99, co. 3, dell'AI Act. Le sanzioni amministrative pecuniarie previste dal GDPR per le più gravi violazioni, prevedono, invece, ex articolo 83, una soglia massima del 4% del "fatturato mondiale annuo".

10 In tal senso sembra deporre anche l'intervento del Segretario Generale IVASS, Dott. De Polis, nel contesto di un Convegno organizzato da Banca d'Italia e ANSPC. Il discorso del Segretario, rammentando vantaggi per le imprese e svantaggi per la clientela dei sistemi di intelligenza artificiale, ha lasciato intendere che la valutazione di norme specifiche sia ancora in itinere. Discorso consultabile al link https://www.ivass.it/media/interviste/intervista/l-intelligenza-artificiale-nel-settore-assicurativo/?dotcache=refresh.

11 Il rischio della prima ipotesi sembra essersi già palesato in importanti paesi *leader* a livello occidentale, ove si è rinunciato alla strutturazione di un corpo legislativo organico in favore, invece, di una delega, più o meno ampia, a normative secondarie. La seconda ipotesi apparrebbe l'unica capace di ridurre a sistema le problematiche applicative dell'operatore di mercato senza perciò attendere le risposte legislative che rischiano di appartenere al mondo del '*perpetual tomorrow*'. Si pensi, ad esempio, agli Stati Uniti d'America ove la volontà di attestarsi quali *leader* nel settore, manifestatasi, pur sotto diverse coloriture, sia nel primo mandato presidenziale di Donald Trump che in quello di Joe Biden, si sia tendenzialmente risolta in una delega vincolata da alcune enunciazioni di principio alle varie agenzie governative, le quali si trovano, ad oggi, sfornite di indicazioni precise sulle modalità applicative da adottare a livello amministrativo.

12 Si vedano, in tema, le considerazioni fatte in OCSE, 'The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector' (2020), consultabile al link https://www.oecd.org/en/topics/finance-and-investment.html.

golati[13].

La necessità di intervenire viene rintracciata dall'Autorità europea nel fatto che più della metà delle imprese assicurative nei rami danni e circa un terzo di quelle che operano nei rami vita parrebbero utilizzare ormai, su base continuativa e per vari stadi della catena del valore, sistemi di IA[14].

Un dato che, tuttavia, può colpire, forse anche in ragione dei timori per una maggiore difficoltà nella gestione delle esternalizzazioni, è il fatto che la maggior parte di queste sembra ancora evitare la fornitura da parte di terzi, prediligendo una strutturazione *in-house* dei sistemi[15]. Tuttavia, la "componentistica" continua, per lo più, a provenire da fuori, ovvero da un oligopolio di fornitori; il che comporta il rischio di concentrazione e di rapida propagazione dei rischi legali ed operativi, richiedendo quindi la strutturazione di apposite pratiche di *governance* e gestione del rischio.

Pur riconoscendo che le previsioni normative e regolamentari del settore continueranno ad applicarsi, EIOPA si propone di intervenire sul fatto che, a causa della loro gestazione in periodi antecedenti all'evoluzione tecnologica più recente, residuerebbero inevitabilmente vuoti sul come declinare o coordinare le vecchie previsioni rispetto al nuovo[16].

Di qui nasce l'interrogativo sul valore aggiunto che l'Autorità ritiene di poter portare. Quesito inscindibilmente legato al dubbio sulla portata realmente innovativa dell'AI Act.

EIOPA, ritenendo che tra gli obiettivi del suo operato rientrino il mantenimento di un mercato interno efficiente e trasparente, con regole e controlli coerenti, la tutela della clientela e la limitazione, attraverso una vigilanza armonizzata, dei rischi nei settori assicurativi e pensionistici, si è chiesta come possano essere assicurate:

1) La mitigazione dei rischi e la massimizzazione dei benefici derivanti dall'IA; e

2) La promozione di buone e convergenti pratiche di vigilanza.

Le ipotesi di offrire linee guida generali fondate sulla normativa esistente o di sviluppare orientamenti dettagliati su casi d'uso o questioni specifiche sono state escluse dal documento di *Impact Assessment* in favore, invece, della strutturazione di una *Opinion* sulla gestione del rischio IA, unica capace di raggiungere i due obiettivi di cui sopra.

Tra i vari benefici di tale approccio para-regolamentare è stata individuata la possibile applicazione di economie di scala nella supervisione dal momento che, nella visione di EIOPA, *"(l)e autorità di vigilanza già controllano il rispetto della normativa assicurativa vigente e dispongono quindi di team in grado di monitorare i rischi relativi a dati, catena di fornitura e modelli, che sono intrinseci ai sistemi di IA"*[17]. Inoltre, poiché "*senza un chiarimento delle aspettative di vigilanza a livello europeo, l'industria rischia di sviluppare pratiche di governance e gestione del rischio (...) omogenee, compromettendo l'obiettivo di garantire condizioni di parità nel mercato*", *"(s)arebbe (...) utile fornire orientamenti su come la normativa settoriale vigente debba essere interpretata nel contesto dell'utilizzo dei sistemi di IA nel settore assicurativo, anche evidenziando aspetti legati (...) al principio di proporzionalità"*[18].

13 Si vedano gli artt. 4, co.2, e 29, co.2, del Regolamento UE n. 1094/2010 (cd. Regolamento EIOPA).

14 EIOPA, 'Report on the Digitalisation of the European Insurance Sector' (30 April 2024), p. 4, consultabile al link https://www.eiopa.europa.eu/document/download/6ca9e171-42b9-44d7-a2e6-beaf0134ecb8_en?filename=Report%20on%20the%20digitalisation%20of%20the%20European%20insurance%20sector.pdf.

15 Sulla questione delle esternalizzazioni e delle crescenti aspettative dei regolatori, si rimanda anche ai rilievi critici effettuati per l'intervento di IVASS a livello nazionale in G.G. Cimini e A. Polizzi, 'Outsourcing nelle assicurazioni: la nuova Lettera al mercato IVASS' *Diritto Bancario* (2025).

16 EIOPA, 'Impact Assessment of Opinion on AI governance and risk management' (6 August 2025), p. 5, consultabile al link https://www.eiopa.europa.eu/document/download/bdd11c63-5f48-442f-8291-598557af44a2_en?filename=Impact%20Assessment%20-%20Opinion%20on%20Artificial%20Intelligence%20governance%20and%20risk%20management.pdf. La formulazione adottata da EIOPA è la seguente: *"(e)xisting sectoral legislation still applies to the use of AI systems in insurance. However, at the time the legislation was approved AI systems did not exist or they were not widely used. In this context, it is important to clarify the application of existing requirements to these new developments and to promote supervisory convergence at European level, amongst other things to reflect risk-based and proportionality considerations"* (Enfasi aggiunta).

17 *Ibidem*, p. 7. (Traduzione dell'autore).

18 *Ibidem*, p. 10. Lo stesso concetto viene rimarcato nel documento laddove, a pagina 11, esplicitamente fa riferimento al fatto che *"(u)n intervento di vigilanza è inoltre giustificato al fine di chiarire i quesiti che i supervisori potrebbero avere riguardo all'applicazione della normativa assicurativa vigente quando le imprese utilizzano sistemi di IA"*. (Traduzione dell'autore).

4. L'opinione di EIOPA e la questione della (reale) autonomia dell'AI Act

Sebbene il Regolamento relativo alle competenze di EIOPA disciplini l'*Opinion* come uno strumento formalmente diretto alle Autorità di vigilanza nazionali, le imprese di assicurazione ne sono il vero convitato di pietra[19].

L'*Opinion* si declina, infatti, su sei punti sensibili che le imprese di assicurazione dovrebbero assicurare disponendo anche un Annex esplicativo in calce al documento. Questi sono "*equità ed etica; governance dei dati; documentazione e conservazione dei registri; trasparenza e spiegabilità; controllo umano; accuratezza, robustezza e cybersicurezza*"[20].

Al termine di due anni dalla pubblicazione, EIOPA effettuerà una ulteriore valutazione sulle prassi di vigilanza che saranno prevalse[21].

4.1 *Equità ed Etica*

L'obbligo in capo alle imprese di assicurazione di agire sempre con equità, la cd. "*fairness*", ed in maniera etica, come ricorda la stessa EIOPA, lungi dall'essere una nuova previsione dell'AI Act, ha il suo fondamento, oltre che nei più antichi principi generali di diritto romano, già nell'art. 17 della Direttiva UE in materia di distribuzione assicurativa (cd. IDD)[22].

19 In particolare risuona con particolare enfasi il monito di EIOPA che, a pagina 7 dell'*Opinion*, sottolinea come le imprese di assicurazione "*(…) sono in ultima analisi responsabili dei sistemi di intelligenza artificiale che utilizzano, indipendentemente dal fatto che tali sistemi siano sviluppati internamente o in collaborazione con fornitori di servizi terzi. Tuttavia, anche i fornitori di servizi terzi hanno un ruolo da svolgere; le imprese dovrebbero ottenere da questi ultimi informazioni e garanzie adeguate riguardo alle caratteristiche, alle capacità, ai dati utilizzati per l'addestramento e il test dei sistemi di IA, nonché alle limitazioni dei sistemi di IA impiegati.*" (Traduzione dell'autore).

20 EIOPA, 'Opinion on AI Governance and Risk Management' (6 August 2025), p. 6 e seguenti, consultabile al link https://www.eiopa.europa.eu/document/download/88342342-a17f-4f88-842f-bf62c93012d6_en?filename=Opinion%20on%20Artificial%20Intelligence%20governance%20and%20risk%20management.pdf

21 *Ibidem*, p. 12.

22 Direttiva UE n. 2016/97. L'articolo impone agli Stati Membri il dovere di garantire che "*(…) nello svolgere l'attività di distribuzione assicurativa, i distributori di prodotti assicurativi agiscano sempre in modo onesto, imparziale e professionale per servire al meglio gli interessi dei loro clienti*" e che "*(…) le comunicazioni di marketing, indirizzate dai distributori di prodotti assicurativi a clienti o potenziali clienti siano imparziali, chiare e non fuorvianti (…)*" e che i distributori "*non offrano un compenso ai loro dipendenti e non ne valutino le prestazioni in modo contrario al loro dovere di agire nel migliore interesse dei clienti*".

Equità ed etica richiamano il controllo o, almeno, la presenza umana oltre che essere ad essa strettamente legati. Perché etica ed equità siano garantiti e non si ci si abbandoni all'azzardo morale della delega è necessaria la presenza della responsabilità umana. È fondamentale infatti per gli insegnamenti di filosofia morale che il controllo umano pervada ogni stadio decisionale poiché, al di là dei fraintendimenti semantici, è utile ricordare, non esistono decisioni autonome intese come riferibili alla macchina, bensì solo automatiche, ovvero, riferibili agli unici soggetti individuabili come autonomi, dunque privi di imposizioni esterne, *i.e.*, gli uomini[23].

Per assicurare ciò l'impresa non ha altra scelta se non l'adozione di politiche interne di governo (umano) dei dati.

4.2 *Governo dei Dati*

Proprio in tema di politiche interne relative alla *governance* dei dati, EIOPA ha voluto rammentare che, già ai sensi del Regolamento Delegato UE n. 2015/35, i processi destinati alla sottoscrizione delle polizze così come quelli attuariali debbono essere portati avanti utilizzando dati sufficienti in quantità oltre che rilevanti ed attendibili[24]. Di analogo tenore risulta la Direttiva UE cd. Solvency II in materia di necessaria accuratezza, completezza ed appropriatezza dei dati utilizzati per il calcolo delle riserve tecniche da accantonare od il Regolamento Delegato UE n. 2017/2358 in tema di test di prodotto[25].

23 Si veda, per una trattazione più ampia, T. M. Powers e J. Ganascia, 'The Ethics of the Ethics of AI' in M. Dubber et al., *Oxford Handbook of Ethics of AI*, (Oxford University Press, 2021). Da questo punto di vista, sebbene il linguaggio utilizzato per riferirsi all'IA ed alle potenzialità della stessa, già a partire dal sostantivo intelligenza, potrebbe indurre a credere, in ultimo luogo, che la macchina od il sistema utilizzato siano soggetti del tutto autonomi dalle decisioni umane, occorre sempre rammentare l'insegnamento iniziale di A. Turing, 'Computing Machinery & Intelligence', Mind (1950). *I.e.*, la macchina è intelligente solo quando riesce ad ingannare l'uomo e fargli credere di essere intelligente, dunque umana, quando, in realtà, è solo automatica, non già autonoma. Un insegnamento utile anche per l'operatore assicurativo, il quale sempre deve ricordarsi che la delega continua ad essere una scelta di cui l'uomo rimane giuridicamente responsabile, anche quando ne discendano decisioni sulle quali non possiede più alcuna capacità di direzione o controllo.

24 Art. 260, co.1, lett. a).

25 Rispettivamente art. 82 Solvency II ed art. 6, co.1, del Regolamento Delegato UE n. 2017/2358.

vedi l'articolo online

Ciò che l'*Opinion* sottolinea, in coerenza con i principi stabiliti dall'AI Act, è la necessità che le informazioni date 'in pasto' al sistema di IA siano storicamente sufficienti, prive di errori e coerenti con l'uso che ne viene fatto.

4.3 *Documentazione e Conservazione*

Il dovere di mantenere copia della documentazione rilevante, oltre che dettato da un principio di prudenza, ormai capace di allargarsi nel tempo per via del sopraggiungere di normative tese a garantire valori sempre più meritevoli di tutela[26], ha il suo fondamento più recente – ricorda l'Autorità UE – nei Regolamenti Delegati UE n. 2015/35 e n. 2017/2358[27].

Questi due atti normativi, in particolare, impongono che le imprese di assicurazione, in vista di *audit* interni, nonché di richieste da parte delle Autorità competenti, si attivino per il mantenimento dei processi che hanno portato in approvazione i propri prodotti, garantendo comprensione, trasparenza e continuità dei presidi. Cionondimeno, in questo contesto, EIOPA si spinge oltre al mero richiamo offrendo una tabella delle tipologie di documenti da conservare e revisionare periodicamente[28].

4.4 *Trasparenza e Spiegabilità*

Sebbene la spiegabilità sia un neologismo di origine giuridico-informatica, la trasparenza, che meno si occupa del rapporto fiduciario che spesso sottende determinati processi decisionali, è di meno recente adozione. La si ritrova già nella Direttiva IDD, laddove si prevede che, prima ancora della stipula del contratto di assicurazione, il distributore debba specificare, basandosi sulle informazioni ottenute dal cliente, le richieste e le esigenze di tale cliente fornendo a questi informazioni oggettive sul prodotto assicurativo in una forma comprensibile al fine di agevolare una decisione informata[29].

Quanto alla spiegabilità, già *leit motiv* dell'AI Act ove si sancisce che "*i sistemi di IA (…) (debbono essere) sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità (…), rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i deployer delle capacità e dei limiti di tale sistema*"[30], EIOPA ha ulteriormente rimarcato che le spiegazioni dovrebbero essere calibrate alle esigenze dei diversi *stakeholders*.

In particolar modo, "*le imprese dovrebbero essere in grado di fornire alle autorità competenti e ai revisori una spiegazione globale e completa sul funzionamento del sistema di intelligenza artificiale. Per i clienti, oltre a essere informati che stanno interagendo con un sistema di IA, su richiesta del cliente dovrebbe essere chiarita l'influenza del sistema di IA sulla decisione che ha un impatto rilevante su di loro, utilizzando un linguaggio semplice, chiaro e non tecnico, in modo da consentire loro di prendere decisioni consapevoli. Ove pertinente, gli intermediari assicurativi dovrebbero inoltre essere informati dalle imprese di assicurazione quando una decisione viene presa sulla base di un sistema di IA, affinché possano adempiere ai propri obblighi legali nei confronti dei clienti*"[31].

4.5 *Controllo Umano*

IVASS ha già avuto modo di chiarire l'anno scorso che un "*(e)ccessivo affidamento agli algoritmi di IA e correlata deresponsabilizzazione della componente umana costituiscono un rischio. In particolare, vanno evitate decisioni automatizzate, specie in situazioni (…) che richiedono il giudizio e la flessibilità decisio-*

26 La preoccupazione forse più diffusa al momento sul mercato riguarda i controlli antiriciclaggio e la conformità alle normative AML. È noto come queste espandano, in maniera talvolta silente, vecchi obblighi di tenuta documentale senza che le relative normative settoriali vengano coerentemente emendate.

27 Rispettivamente all'art. 258, co. 1, lett. i) ed all'art. 9.

28 L'Allegato I all'*Opinion* offre undici tipologie. I documenti che si potrebbero definire di maggiore interesse sono, ad esempio, quelli che attestano le ragioni per le quali si è deciso, con debito sistema di *audit*, di utilizzare sistemi di IA, insieme alla sezione nella quale si richiede di "*documentare le motivazioni per cui è stato scelto un determinato tipo di algoritmo di intelligenza artificiale rispetto ad altri, nonché le librerie associate con i relativi riferimenti esatti*" e di registrare, spiegare e giustificare "*i trade-off etici, di trasparenza e spiegabilità*" (pp. 14-15). (Traduzione dell'autore).

29 Cfr. Art. 20, co.1. L'*Opinion* specifica inoltre che simili e più dettagliati obblighi sono rinvenibili in tema all'art. 258 lett. h) del Regolamento Delegato UE n. 2015/35 ed all'art. 8 del Regolamento Delegato UE n. 2017/2358.

30 Considerando n. 27 dell'AI Act.

31 EIOPA, 'Opinion on AI Governance and Risk Management' (6 August 2025), p. 10 e seguenti, consultabile al link https://www.eiopa.europa.eu/document/download/88342342-a17f-4f88-842f-bf62c93012d6_en?filename=Opinion%20on%20Artificial%20Intelligence%20governance%20and%20risk%20management.pdf. (Traduzione dell'autore).

nale tipica delle potenzialità cognitive umane"[32].

Poiché, come visto in tema di etica ed equità, spiegabilità e trasparenza presuppongono una forma di controllo umano ed è compito dell'organizzazione (di uomini) valutare, monitorare, testare, gestire ed assumersi la responsabilità per i rischi associati alla tecnologia utilizzata, nonché proteggere quest'ultima da ipotesi di uso improprio, se di errore nel processo informatico si parlerà, dunque, questo non potrà che essere, in ultima istanza, umano. Analogo ragionamento sulla gestione dei rischi e sulla continua responsabilità deve essere fatto per il comune caso di sistemi di IA provenienti da fornitori terzi[33].

L'*Opinion* di EIOPA, richiamandosi al già esistente art. 46 di Solvency II ed ai già citati Regolamenti Delegati[34], fuga ogni residuale dubbio circa la necessità che le imprese di assicurazione, per assicurare il celebre *human in the loop*, debbano disporre di controlli interni ad ogni livello anche e soprattutto se le attività sono esternalizzate. In particolare, le responsabilità devono essere allocate tra i membri dell'organo amministrativo, di gestione o di supervisione, i quali devono essere ritenuti responsabili dell'utilizzo complessivo dei sistemi di IA all'interno dell'organizzazione e devono possedere una conoscenza adeguata del modo in cui tali sistemi vengono utilizzati e dei potenziali rischi connessi[35].

32 IVASS, 'L'intelligenza artificiale nel settore assicurativo' *Convegno Banca d'Italia Milano e ANSPC: "Intelligenza artificiale e mondo finanziario: quali applicazioni, quali implicazioni"* (Milano, 9 ottobre 2024), p. 4, consultabile al link https://www.ivass.it/media/interviste/documenti/interventi/2024/2024_10_09_sdp_ai_bkimi_anspc/SDP_Convegno_IA _09.10.2024.pdf.

33 Si veda, in particolare, l'art. 28 del DORA in materia di gestione di rischi presso terzi.

34 Regolamenti Delegati UE n. 2015/35 e n. 2017/2358.

35 Sul tema si rimanda a anche alle osservazioni espresse in The Geneva Association, 'Regulation of Artificial Intelligence in Insurance – Balancing Consumer Protection and Innovation' (Settembre 2023), consultabile al link https://www.genevaassociation.org/publication/public-policy-and-regulation/regulation-artificial-intelligence-insurance-balancing. Benché da un mero punto di vista di gestione societaria, l'avvento dei sistemi di IA nulla muterebbe rispetto alle prerogative decisionali del *Board* della compagnia, il cambiamento concerne la ideale distanza tra lo stesso consiglio di amministrazione ed il cliente finale, ormai caratterizzata da una allungata catena di gestori che si affideranno a sviluppatori, i cd. *developers*, cui seguirà, nel rapporto diretto con il cliente, una *front-line* molto probabilmente automatizzata. Lo spazio di monitoraggio e di controllo si fa, dunque, più ampio, ma l'origine ultima del processo decisionale permane umana, in linea peraltro con l'approccio antropocentrico che pervade, seppur in maniera distinta, tutte le moderne legislazioni in materia, ed in linea con le indicazioni provenienti dall'etica dell'IA. Si veda, per una trattazione più approfondita, M. Dubber et al., 'Oxford Handbook of Ethics of AI', (Oxford University Press, 2021).

A questi soggetti si aggiungono le funzioni fondamentali di conformità e di *audit*, incaricate di verificare che l'utilizzo dei sistemi di IA all'interno della singola compagnia e di un gruppo assicurativo sia conforme a tutte le leggi e normative applicabili. Il Responsabile della Protezione dei Dati deve, poi, verificare che i dati personali trattati dai sistemi di intelligenza artificiale siano gestiti in conformità con le normative vigenti in materia di protezione dei dati. Infine, la funzione attuariale deve essere responsabile per i controlli sui sistemi di IA che rientrano nelle proprie competenze, *e.g.*, per il coordinamento del calcolo delle riserve tecniche o per il parere sulla politica di sottoscrizione.

4.6 *Accuratezza, Robustezza e Cybersicurezza*

Infine, anche in merito alla cd. cybersicurezza, le linee guida possono essere desunte dall'art. 46 di Solvency II relativo ai sistemi di controllo interno come recentemente specificate dal Regolamento DORA, il quale richiede che le imprese dispongano di piani per la gestione dei rischi ICT solidi, completi e ben documentati, predisponendo requisiti uniformi, attuando, mantenendo e testando piani di continuità operativa e di emergenza (i cd. *fall-back plans*)[36].

5. Osservazioni conclusive

In definitiva, l'*Opinion* di EIOPA sembrerebbe rappresentare più un esercizio di sistematizzazione che un reale passo avanti nella regolamentazione del rischio IA.

Pur offrendo chiarezza interpretativa e rafforzando la coerenza tra AI Act e disciplina assicurativa, l'intervento si muove ancora (comprensibilmente) entro i confini delle regole esistenti, non potendo proporre *standard* realmente innovativi o settoriali, che dovranno trovare un convergere di intenti e sforzi che non possono richiedersi a un'iniziativa solo di EIOPA.

Ne emerge l'impressione di un approccio ancora necessariamente prudente, volto a contenere l'incertezza e a rammentare le regole di "buon senso" declinate per il settore assicurativo.

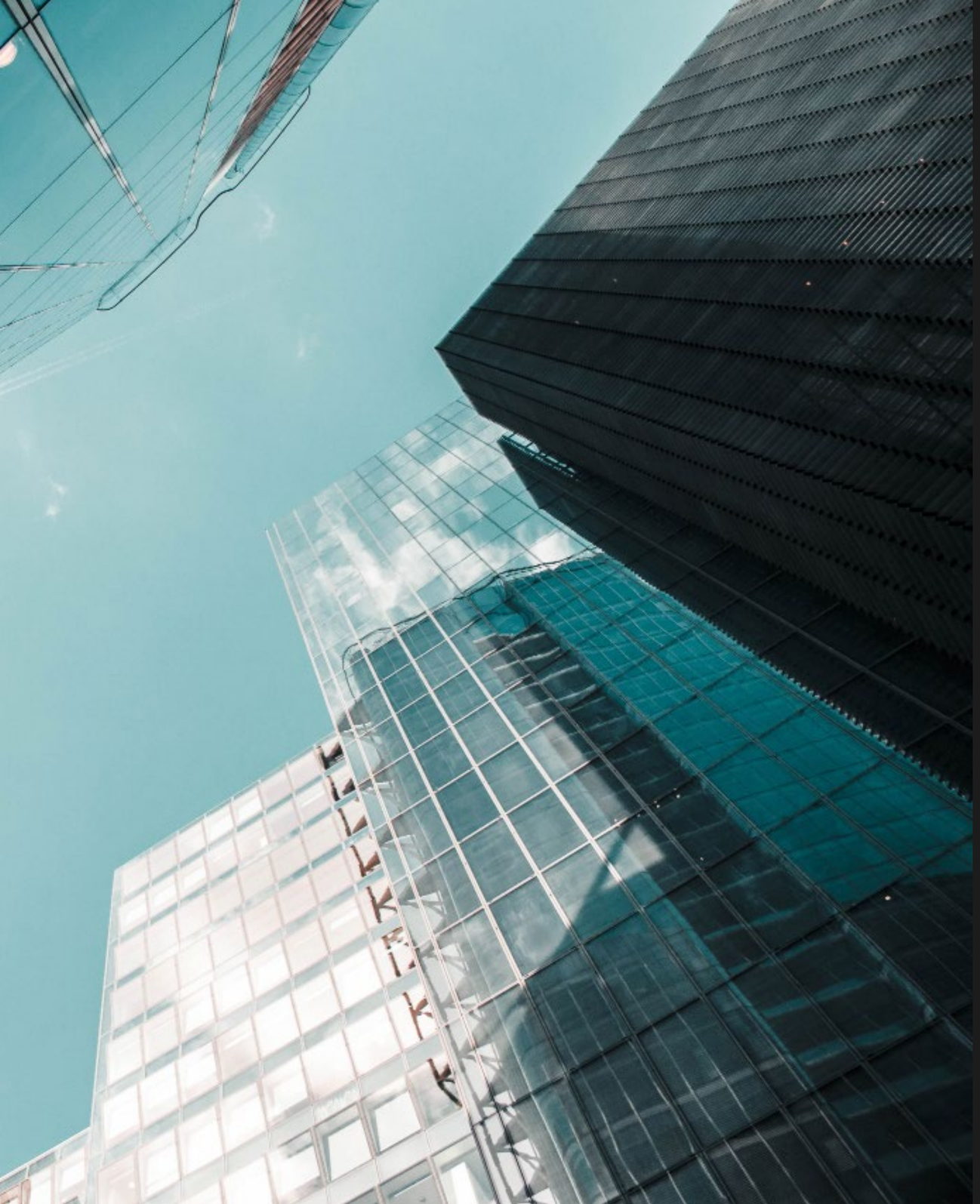
Resta aperta la più ampia questione su quanto l'Europa possa o sia in grado davvero di incidere, e non

36 Cfr. Artt. 6, 7, 8, 9, 10, 11 e 12 di DORA.

vedi l'articolo online

solo ordinare, rispetto al futuro della *governance* dell'intelligenza artificiale.

vedi l'articolo online



DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it