IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

La Vigilanza assicurativa nel contesto dell'evoluzione tecnologica e della sostenibilità

Intervento di

Stefano De Polis - Segretario Generale IVASS

Fondazione CESIFIN - AIDA Toscana - Convegno "La vigilanza del mercato assicurativo di fronte all'evoluzione tecnologica e al principio di sostenibilità"

Firenze, 7 febbraio 2025

Ringrazio la Fondazione Cesifin e l'AIDA Toscana per l'invito a partecipare a questo convegno che intende avviare una riflessione su talune significative novità che interessano la vigilanza assicurativa; per conseguire al meglio nel tempo le proprie finalità la vigilanza deve alcune volte stimolare, altre volte accompagnare i cambiamenti del contesto di riferimento. E' un processo fisiologico; è però importante chiedersi se e come i mutamenti influiscano sui connotati della funzione in termini di finalità, assetti e processi.

La vigilanza assicurativa delineata dal Codice delle Assicurazioni Private prevede un utilizzo integrato di regole, flussi di informazioni e una verifica continua del corretto esercizio dell'attività delle imprese e degli intermediari (cfr. fig. 1, allegata). In sintesi, un insieme integrato di vigilanza regolamentare, informativa, e ispettiva (quest'ultima intesa in senso lato), volto a perseguire la sana e prudente gestione delle compagnie e al contempo a promuovere comportamenti corretti e trasparenti nei confronti della clientela (CAP artt. 3 e 3 bis).

Le norme settoriali introducono specifiche e calzanti regole di *governance*, organizzative, prudenziali, di gestione delle crisi[1] e di tutela della clientela. Un sistema di segnalazioni periodiche, integrato da fonti pubbliche, dai reclami e all'occorrenza da richieste *ad hoc*,

[1] Si veda anche S. De Polis, *La vigilanza creditizia nel sistema di Corporate Governance*, in Banche e Banchieri 1997, n. 1, in particolare pp. 29-31.

permette di disporre dei dati, delle informazioni e delle valutazioni necessarie alle attività di controllo.

L'efficace combinazione di attività professionali di controllo a distanza e ispettive, questa volta in senso stretto, rende possibile monitorare e verificare nel tempo la qualità dei dati, l'osservanza delle disposizioni e il corretto esercizio dell'attività assicurativa. Le valutazioni che ne conseguono da parte degli Uffici possono dare il via a confronti dialettici e interventi correttivi, anche sanzionatori, nei confronti delle imprese.

Tuttavia, se norme e flussi informativi sono in larga parte armonizzati a livello europeo, cioè hanno struttura e contenuti nel complesso allineati, l'attività di supervisione è al momento meno omogenea in termini di sistematicità e intensità degli approcci nell'ambito dei diversi Stati membri.

L'IVASS, in linea con una consolidata cultura della vigilanza in Italia, ha sempre riservato, nei limiti delle risorse disponibili, attenzione per l'efficacia e la pervasività dell'assetto dei controlli, anche ispettivi, che devono essere in grado all'occorrenza di valutare, mediante una pertinente azione di *intelligence* dei comportamenti, dei dati e delle informazioni, le singole situazioni aziendali in termini di corretta gestione e i *trend* del sistema.

Tuttavia, gli ambiti e i profili di rischio con cui si misura l'attività di vigilanza si evolvono. Mi riferisco all'esigenza di governare opportunità e rischi delle nuove tecnologie, ai temi della sostenibilità, alle esigenze di azione coordinata a livello europeo. È un contesto sfidante, anche in termini di risorse e competenze.

Prima di affrontare le prospettive della vigilanza assicurativa di fronte ai rischi dell'evoluzione digitale e al principio di sostenibilità, vorrei soffermarmi brevemente su un nuovo ambito di azione.

Da domani, 8 febbraio, l'IVASS, analogamente ad altre Autorità di settore, darà avvio ai 'controlli rafforzati' previsti legge 9 dicembre 2021, n. 220 sulla corretta applicazione da parte delle compagnie del divieto di finanziamento delle società produttrici di mine antiuomo e di bombe a grappolo messe al bando dai trattati di Ottawa e Oslo. Si tratta di una nuova attività; presto saranno svolte le prime verifiche. Trattandosi di un compito di controllo la cui *ratio* va ricercata nella volontà del Legislatore di assicurare il rispetto degli accordi internazionali sottoscritti dal Paese, esso sembra rientrare nella generale verifica del corretto adempimento degli obblighi di *compliance* da parte delle compagnie. Si tratta indubbiamente di un compito particolare.

Vigilanza e rischi dell'evoluzione tecnologica. L'intelligenza artificiale, in via crescente generativa, aumenta in modo esponenziale le potenzialità di utilizzo dei dati e la necessità di un governo integrato dell'innovazione tecnologica. L'interesse pubblico, in un'ottica di tutela degli assicurati, è capitalizzare i benefici di questa evoluzione senza compromettere la tutela degli utenti finali e la piena affidabilità e funzionalità del sistema assicurativo.

L'Artificial Intelligence Act prevede specifiche forme di tutela preventiva e di vigilanza volte a garantire i diritti fondamentali di chi entra in contatto con i sistemi di IA: l'enfasi è sui sistemi ad alto rischio di violazione dei diritti fondamentali. Considerato che le norme in tema di IA lasciano impregiudicate le regole settoriali già previste per la stabilità delle imprese e del sistema nonché a protezione dei consumatori, si sta lavorando a livello europeo e nazionale per garantire una vigilanza ad ampio spettro e per evitare duplicazione degli oneri.

In questo contesto è importante il pieno e diretto coinvolgimento delle Autorità di controllo dei diversi settori finanziari anche nella sorveglianza dei sistemi di IA dei soggetti vigilati. Si tratta di una attività che richiede professionalità specifiche, allo stato da formare, ma sono evidenti le sinergie con le funzioni di vigilanza sia prudenziale, attenta alla gestione dei rischi, sia di condotta e tutela, orientate alla protezione sostanziale dei consumatori. L'IVASS sta collaborando con le altre Autorità di settore e i Ministeri competenti alla predisposizione del quadro normativo nazionale applicativo dell'architettura europea. In ambito EIOPA si stanno definendo i principi per una applicazione omogenea ed integrata della regolamentazione.

Dal 17 gennaio 2025 è applicabile il Regolamento sulla resilienza operativa digitale del settore finanziario (*Digital Operational Resilience Act*, DORA), che introduce norme armonizzate a livello europeo in materia di gestione dei rischi legati all'utilizzo della tecnologia dell'informazione e della comunicazione (ICT). Il Regolamento rafforza presìdi già presenti nella normativa, anche italiana (Reg. IVASS 38/2018), che devono essere adottati da compagnie e grandi intermediari per prevenire e gestire i rischi connessi all'utilizzo delle tecnologie digitali e ne introduce ulteriori del tutto innovativi.

L'ICT permea ormai l'intera operatività delle compagnie e degli intermediari, esponendo gli operatori a nuovi, rilevanti rischi a causa della complessa rete di connessione tra sistemi informatici delle compagnie, dei *provider* di informazioni, dei fornitori di servizi di gestione

delle infrastrutture informatiche. Il crescente e massiccio ricorso all'esternalizzazione di funzioni di elaborazione dati, di gestione delle piattaforme tecnologiche e di sviluppo delle applicazioni aziendali verso operatori specializzati è ormai parte integrante della catena del valore dei servizi finanziari e quindi fondamentale per la stabilità e l'integrità delle imprese e per la stessa resilienza del sistema. Questa tendenza porta a una crescente probabilità e impatto di incidenti cibernetici, in aumento nell'ultimo triennio.

L'IVASS ha avviato da tempo diverse attività in materia di sicurezza cibernetica delle compagnie e degli intermediari assicurativi italiani: esse si articolano in iniziative di sensibilizzazione, in accessi ispettivi specialistici e in test avanzati di sicurezza cibernetica di tipo *Threat-Led Penetration Testing* – parte del progetto TIBER-EU – per rafforzare la resilienza informatica delle singole entità e, per tale via, del sistema finanziario nel suo complesso.

Nel 2024 per sensibilizzare le compagnie l'IVASS ha chiesto un'autovalutazione sul livello di conformità a quanto richiesto dal Regolamento DORA. Il mercato assicurativo è consapevole del lavoro da svolgere per raggiungere gli *standard* richiesti, in particolare per quanto riguarda la definizione da parte delle imprese della propria strategia di resilienza digitale e la revisione degli accordi contrattuali con fornitori terzi di servizi ICT.

L'importanza di presidiare le scelte strategiche e i rischi connessi alla esternalizzazione dei servizi ICT a fornitori terzi è una delle quattro aspettative indicate dall'IVASS nella recente pubblica consultazione di una lettera con la quale si vuole richiamare l'attenzione del mercato sul tema dell'*outsourcing* di attività essenziali e importanti.

Il vero elemento di novità del Regolamento DORA risiede nel riconoscimento della ormai avvenuta "globalizzazione delle sfide tecnologiche". Esso introduce un quadro di sorveglianza e monitoraggio costante delle attività dei fornitori terzi di servizi ICT considerati critici a livello europeo. Il Regolamento ha definito un sistema di sorveglianza basato su un'articolata ripartizione di compiti e responsabilità tra Autorità nazionali e unionali, fermo restando che non si tratta di una vigilanza prudenziale a fini di stabilità di tali operatori, la cui attività non è oggetto di riserve legislative, né soggetta a preventiva autorizzazione e di conseguenza neppure a misure di salvaguardia.

Il Regolamento DORA e le relative norme di attuazione affidano la responsabilità e i poteri di sorveglianza sui c.d. *critical ICT third-party service providers* (CTPPs) a livello europeo – identificati sulla base di rilevazioni periodiche sugli *outsourcer* nei mercati assicurativo,

bancario e finanziario - a un'Autorità di vigilanza capofila designata tra EBA, ESMA ed EIOPA in base al settore finanziario prevalentemente servito dal fornitore terzo[2]. Operativamente le attività di supervisione *on-site* e *off-site* (indagini, ispezioni, raccomandazioni per l'efficace gestione del rischio informatico) verranno svolte da *Joint examination team* costituiti da personale delle tre Autorità europee e da risorse messe a disposizione dalle singole Autorità nazionali con competenze specifiche per la gestione dei rischi operativi e informatici[3].

Nel modello descritto, le Autorità nazionali di vigilanza, quali l'IVASS, contribuiscono all'attuazione dell'attività di sorveglianza. Esse inoltre si interfacciano con le imprese vigilate (nel nostro caso le compagnie e i grandi intermediari italiani) per rappresentare le criticità identificate nelle raccomandazioni dell'Autorità di vigilanza europea capofila ai fornitori terzi critici e valutare l'efficacia delle iniziative assunte dalle entità finanziarie. In caso di rischi per la sana e prudente gestione, l'IVASS potrà attivare i propri poteri di intervento che possono arrivare a richiedere alle imprese vigilate la modifica o la rescissione del contratto di fornitura dei servizi ICT.

Siamo in presenza di un ulteriore modello di supervisione: le ESA valutano la gestione dei rischi informatici da parte dei CTPPs e le Autorità nazionali intervengono all'occorrenza sulle imprese vigilate che si avvalgono dei servizi di tali *outsourcer* a salvaguardia della resilienza dei singoli operatori e del sistema finanziario nel suo complesso. La validità del modello e quindi l'efficacia dell'azione di sorveglianza/vigilanza dipenderà in larga misura dall'interazione tra le ESA e le Autorità nazionali.

Vigilanza e sostenibilità ESG. Il settore assicurativo riveste un'importanza cruciale per la realizzazione delle politiche ESG, in ragione sia dell'offerta di protezione a fronte dei rischi fisici connessi con il cambiamento climatico, sia del ruolo che svolge in qualità di investitore istituzionale e nell'offerta di prodotti di investimento sostenibili.

In materia di finanza sostenibile il legislatore europeo ha emanato nell'ultimo quinquennio norme complesse, tra loro interconnesse, che interessano trasversalmente i vari settori dell'economia reale, oltre al settore finanziario: si pensi alla *Sustainable Finance Disclosure*

[2] Il *Board of Supervisors* dell'Autorità di vigilanza capofila approva tutti gli atti e le decisioni relative ai fornitori terzi critici soggetti alla sua supervisione (incluse le sanzioni).

[3] Il quadro organizzativo unionale prevede altresì strutture di coordinamento intersettoriali, chiamate tra l'altro a individuare i fornitori terzi critici, e di coordinamento operativo.

Regulation (SFDR) del 2019, al Regolamento Tassonomia del 2020, alla Direttiva CSR(D) del 2022 sulla rendicontazione non finanziaria, alla più recente Direttiva 2024/1760 (*Corporate Sustainability Due Diligence Directive* - CSDDD[4]) sul dovere di diligenza delle grandi imprese. Sugli stessi temi modifiche sono state apportate alle regolamentazioni chiave del settore assicurativo: *Solvency II* e IDD[5].

Di fronte a queste rilevanti innovazioni l'IVASS ha agito, come di consueto, su un doppio fronte.

In primo luogo l'Istituto ha adeguato la normativa secondaria, integrando i temi di sostenibilità nella *governance* delle imprese di assicurazione, nei processi di POG e nelle regole di comportamento e consulenza in materia di prodotti IBIP.

Contestualmente sono state avviate indagini sistematiche per valutare come le imprese assicurative adeguano i processi di governo, l'informativa al mercato, gli investimenti e i prodotti alle novità regolamentari. Nel 2022 ha preso le mosse una rilevazione annuale dei rischi da catastrofi naturali e di sostenibilità che coinvolge tutte le compagnie che operano in Italia. Il monitoraggio vuole contribuire a una migliore comprensione del ruolo delle assicurazioni nella riduzione del gap di protezione e nella transizione verso un'economia sostenibile. Esso è in grado di raccogliere informazioni strutturate sui rischi ESG del settore assicurativo anche grazie alla scelta di orientare le imprese verso criteri omogenei di rilevazione dei dati, limitando i margini di indeterminatezza esistenti. Proprio per la novità di questa rilevazione, la Commissione Europea ha coinvolto l'IVASS in un progetto per la definizione di un set comune di dati a livello europeo.

Ma il quadro normativo unionale è in ulteriore evoluzione: è recente l'annuncio della Commissione Europea di procedere a consolidare in una regolamentazione c.d. *Omnibus* buona parte dei Regolamenti e delle Direttive richiamate; l'obiettivo è quello di ridurre il *regulatory burden* per gli operatori economici, ritenuto da più parti eccessivo, procedendo a una razionalizzazione e semplificazione del quadro normativo.

° ° °

[4] La CSDDD introduce per le società con più di mille dipendenti e un fatturato superiore a 450 milioni di euro un dovere di diligenza nel promuovere un comportamento aziendale sostenibile e responsabile sotto il profilo ambientale e sociale lungo l'intero processo di produzione e distribuzione. La direttiva richiede agli Stati membri di designare una o più autorità di controllo e introduce anche, a salvaguardia dei diritti umani e dell'ambiente, una responsabilità civile delle imprese per i danni causati.

[5] Il Reg. del. (UE) n. 2021/1256 ha modificato il Reg. del. n. 2015/35 (Solvency II); il Reg. del. (UE) n. 2021/1257 ha modificato i Regolamenti delegati (UE) 2017/2358 e (UE) 2017/2359 (IDD, POG e condotta nella distribuzione).

Concludo con un contributo per le riflessioni.

Finalità, regole, assetto dei controlli, proporzionalità, evoluzione del contesto esterno calibrano l'efficacia della vigilanza (assicurativa). Permane un potenziale rischio residuale; è compito del legislatore delineare il quadro per gestirlo, contemperando obiettivi di *policy*, economia di mercato, equità.

L'evoluzione normativa intervenuta negli ultimi anni, penso in particolare alle due Direttive di riferimento per il settore assicurativo (*Solvency II* e IDD), ha confermato la centralità degli assicurati e degli aventi diritto alle prestazioni assicurative, la cui adeguata protezione è l'obiettivo della vigilanza assicurativa; a tal fine – recita l'art. 3 del CAP - l'IVASS persegue la sana e prudente gestione e la corretta condotta di mercato degli operatori.

Nella fase che stiamo vivendo l'azione di vigilanza tende ad ampliarsi sino a ricomprendere la capacità dei soggetti vigilati di adattarsi in modo resiliente alle sfide poste dall'innovazione tecnologica e alle esigenze di uno sviluppo sostenibile.

I cambiamenti della società, della tecnologia, del clima del pianeta e il mutamento degli scenari geopolitici sono all'origine dei nuovi compiti delle autorità di vigilanza del settore finanziario; per adempiere agli stessi sono richiesti significativi investimenti in risorse professionali, manageriali e organizzative, benché le normative prevedano ormai costantemente che le nuove attività siano svolte a invarianza di risorse umane e di oneri per il bilancio dello Stato.

E' pertanto fondamentale che tra i controlli demandati ad una stessa Autorità ci siano solide sinergie di scala e di scopo, affinché si preservi la razionalità e la funzionalità del modello di vigilanza. I più recenti interventi normativi in materia di sostenibilità – mi riferisco in particolare alla CSDDD – sembrano connotare la sostenibilità come parte integrante dello *statuto* delle grandi imprese europee, anche finanziarie e assicurative. Si potrebbe pertanto configurare l'attribuzione alle autorità di vigilanza del settore finanziario di una nuova finalità: il perseguimento della sostenibilità ESG dei soggetti vigilati tenuti all'obbligo di *due diligence*. E' un tema avvincente, di sapore quasi "filosofico": torneremo a parlarne definito il progetto *Omnibus*.

Figura 1

SCHEMA DI FUNZIONAMENTO DELLA VIGILANZA ASSICURATIVA