13

COLLANA DEL
DIPARTIMENTO
DI ECONOMIA
AZIENDALE

A cura del

COMPLIANCE LAB

REGOLAMENTAZIONE E INNOVAZIONE

Compliance motore di sviluppo e sfida strategica per la crescita aziendale

Roma TrE-Press
2026

Roma Tre
Università degli Studi Roma Tre
Dipartimento di Economia aziendale

DECA Collana del Dipartimento di Economia Aziendale

1 *Analisi di bilancio. Un percorso di sintesi*
Marco Tutino

2 *Sindacati in un mondo globale*
Giampiero Bianchi

3 *Ideazione, sviluppo e marketing dei nuovi prodotti*
Carlo A. Pratesi, Andrea Geremicca

4 *Studi e ricerche del Dipartimento di Economia Aziendale 2023*
a cura di Alberto Pezzi

5 *Il consumatore: responsabile, attivo, partecipativo*
a cura di Fabio Bassan, Maddalena Rabitti

6 *Profili ragionieristici della contabilità nazionale*
Claudio Columbano

7 *Investment advice and sustainability. A survey on professional-client interactions*
Paola Soccorso, Massimo Caratelli

8 *Studi e ricerche del Dipartimento di Economia Aziendale 2024*
a cura di Alberto Pezzi

9 *Qualità, Innovazione e Sostenibilità nella filiera agro-alimentare*
a cura di Maria Claudia Lucchetti, Maria Francesca Renzi

10 *L'applicazione dell'AI Act in Italia e la tutela del consumatore*
a cura di Maddalena Rabitti, Fabio Bassan

11 *Marketing e innovazione*
Carlo Alberto Pratesi

12 *Piattaforme digitali e consumatori: il ruolo delle attività indipendenti*
a cura di Fabio Bassan

Università degli Studi Roma Tre
Dipartimento di Economia Aziendale

13

COLLANA DEL DIPARTIMENTO
DI ECONOMIA AZIENDALE

REGOLAMENTAZIONE E INNOVAZIONE

Compliance motore di sviluppo e sfida strategica per la crescita aziendale

A cura del
COMPLIANCE LAB

RomaTrE-Press
2026

Collana del Dipartimento di Economia Aziendale
Direttore
Alberto Pezzi

Coordinamento editoriale
Gruppo di Lavoro *Roma TrE-Press*

Impaginazione e cura editoriale
teseo editore Roma teseoeditore.it

Elaborazione grafica della copertina
MOSQUITO mosquitoroma.it

Edizioni Roma TrE-Press ©
Roma, giugno 2026
ISBN: 979-12-5977-642-6

http://romatrepress.uniroma3.it

L'attività della *Roma TrE-Press* è svolta nell'ambito della
Fondazione Roma Tre-Education, piazza della Repubblica 10, 00185 Roma.

IL PROGETTO ROMA TRE-PRESS

Il progetto della Roma TrE-Press nasce nel 2013 ed inizia la sua attività all'interno del Sistema Bibliotecario di Ateneo.

Vengono avviate le prime Collane e Riviste di Ateneo. Fin dall'inizio il progetto ha scelto la strada dell'open access: opere scientifiche realizzate in formato digitale ed accessibili a chiunque, dovunque, sempre.

Le ragioni sono le stesse che spingono altre università europee: la ricerca accademica è finanziata da risorse pubbliche; occorre che i suoi risultati siano accessibili a tutti, senza onerose intermediazioni; ciò è reso possibile dalle tecnologie digitali; rientra nella "terza missione" delle università diffondere al pubblico più largo i suoi prodotti sia didattici che scientifici; ma è anche un'esigenza di contenimento dei costi dettata dalle crescenti ristrettezze di bilancio.

Nel primo quinquennio (2013/2017) la Roma TrE-Press pubblica quasi 100 volumi. La crescente richiesta dei ricercatori dell'Ateneo e il successo dell'iniziativa (oltre 150.000 downloads) suggeriscono agli organi di Ateneo di affidare, a partire dall'autunno 2018, l'attività di e-press alla Fondazione Roma Tre Education.

Le linee guida della Roma TrE-Press sono:

• La piena autonomia scientifica dei Dipartimenti e dei Centri di Ateneo nella scelta di che cosa pubblicare, con un forte incoraggiamento verso procedure di assicurazione della qualità secondo le migliori prassi recepite dalle comunità scientifiche di riferimento.

• L'apertura verso autori e istituzioni non appartenenti all'Università Roma Tre, secondo logiche di aggregazione e di promozione della ricerca di qualità.

• Il plurilinguismo, non solo come esigenza culturale ma anche come strumento di coesione e collaborazione internazionale.

• La cura – affidata alla responsabilità della Roma TrE-Press – della linea grafica (copertine e impaginazione), secondo la secolare tradizione del libro come prodotto anche estetico ed artistico.

• La promozione del movimento verso una generale politica di open access che coinvolga anche altre istituzioni accademiche italiane e straniere in coerenza con il dettato dell'art. 9 della nostra Costituzione: "*La Repubblica promuove lo sviluppo della cultura e la ricerca scientifica e tecnica*".

Università degli Studi Roma Tre
Dipartimento di Economia Aziendale
Codice etico delle Colane edite da Roma Tre Press

Il Dipartimento di Economia Aziendale per le collane edite da Roma TrE-Press si impegna a garantire standard di comportamento etico in ogni fase del processo editoriale, ispirandosi alle linee guida del **Committee on Publication Ethics (COPE)**.

1. Doveri degli Autori

- **Originalità e Proprietà Intellettuale:** gli autori garantiscono che l'opera sia originale e non violi i diritti di proprietà intellettuale di terzi. Devono citare correttamente ogni fonte per evitare il plagio e ottenere i permessi per riprodurre contenuti protetti da copyright.
- **Paternità dell'opera:** L'elenco degli autori deve riflettere accuratamente chi ha svolto la ricerca. In caso di paternità multipla, l'ordine dei nomi è determinato congiuntamente dai coautori.
- **Uso dell'Intelligenza Artificiale (IA):** gli strumenti di IA non possono essere indicati come autori o co-autori.
  - È consentito l'uso di IA esclusivamente per finalità di supporto tecnico (es. traduzione, miglioramento della fluidità linguistica, correzione grammaticale e rielaborazione stilistica).
  - È vietato l'uso di IA per la generazione di contenuti scientifici originali, interpretazione di dati o formulazione di conclusioni.
  - Gli autori devono dichiarare esplicitamente nel manoscritto (es. in una nota o nei ringraziamenti) l'impiego di tali strumenti, specificandone il modello e le finalità. L'autore umano resta l'unico responsabile dell'accuratezza e dell'integrità del lavoro.
- **Esclusività:** I manoscritti non devono essere inviati contemporaneamente ad altri editori.
- **Finanziamenti e Conflitti di Interesse:** Eventuali fonti di finanziamento della ricerca e conflitti di interesse devono essere chiaramente identificati nel manoscritto.

2. Doveri del Direttore e dei Comitati (Scientifico ed Editoriale)

- **Imparzialità ed Equità:** Le decisioni si basano esclusivamente sulla qualità scientifica e
l'idoneità del lavoro per la Collana, senza discriminazioni di alcun tipo.
- **Trasparenza del Processo:** Il Comitato Editoriale supervisiona il referaggio garantendo l'anonimato tra autori e revisori.
- **Gestione dei Conflitti d'Interesse:** In caso di contributi proposti da membri del Comitato Editoriale, la gestione della pratica è affidata esclusivamente al Direttore per garantire l'assoluta terzietà.
- **Riservatezza:** Tutto il materiale ricevuto deve essere trattato come riservato fino alla pubblicazione.

3. Doveri dei Revisori (Referee)

- **Oggettività e Qualità:** I revisori devono valutare il materiale con cura e obiettività, fornendo feedback costruttivi in modo tempestivo.
- **Conflitto di Interessi e Riservatezza:** I revisori devono segnalare immediatamente qualsiasi conflitto di interessi. Non possono utilizzare per fini personali le informazioni contenute nei manoscritti né generare il report caricando i lavori su piattaforme di IA generativa.
- **Segnalazione di Irregolarità:** I revisori sono tenuti a informare il Direttore in caso di sospetto plagio o somiglianze eccessive con opere già edite. Il Direttore e il Comitato Editoriale avviano un'indagine interna. Qualora l'indagine confermi comportamenti scorretti, la Collana provvederà al ritiro dell'opera dalla piattaforma Roma TrE-Press o alla pubblicazione di una errata corrige ufficiale.

Collana del Dipartimento di Economia Aziendale

Editorial Policy e descrizione dello scopo della Collana

La collana nasce con lo scopo di contribuire allo sviluppo e alla diffusione delle tematiche di gestione d'impresa: economico-aziendali, finanziarie, giuridiche e matematiche, valorizzando il pluralismo culturale e l'interdisciplinarietà presenti nel Dipartimento.

La collana è aperta a contributi che supportino il miglioramento della didattica dei corsi di studio universitari e post-universitari e favoriscano il dibattito tra il modo delle imprese e il mondo accademico.

La collana accoglie contributi monografici e collettanee.

I volumi pubblicati nella collana sono sottoposti a referaggio affidato al Comitato editoriale.

I volumi pubblicati dalla collana sono liberamente accessibili in formato elettronico sul sito dell'editore Roma TrE-Press. La versione a stampa è acquistabile in modalità "Print on demand".

Le pubblicazioni hanno una numerazione progressiva ed eventuali richiami o citazioni ad essi devono riportare la denominazione estesa del contributo a cui si fa riferimento.

AUTORI

Piero BOCCASSINO
Senior Advisor del CEO e già Chief Compliance Officer – Gruppo Intesa Sanpaolo

Claudio CLEMENTE
Già Direttore dell'UIF - Unità di Informazione Finanziaria per l'Italia e Presidente Onorario AICOM – Associazione Italiana Compliance

Antonio GRAZIANO
Responsabile Antiriciclaggio – Gruppo Poste Italiane

Francesco MAURO
Head of Unit Supervisory Review, Recovery and Resolution – EBA

Ida MERCANTI
Segretario Generale IVASS

Raffaele PANÌCO
Risk & Compliance Officer – Gruppo Poste Italiane

Alberto PEZZI
Professore Ordinario di Economia e gestione delle imprese - Università degli Studi Roma Tre

Massimo RELLA
Direttore Crediti – Banca Mediolanum

Marco ROSSETTI
Group Chief Compliance Officer – Banca Mediolanum

Enzo SERATA
Direttore dell'UIF - Unità di Informazione Finanziaria per l'Italia

Giuseppe SIANI
Capo del Dipartimento Vigilanza bancaria e finanziaria della Banca d'Italia

Andrea TURI
Responsabile della Divisione Vigilanza Intermediari e Protezione Investitori - Consob

Silvia VICENTINI
Vice Presidente AICOM - Associazione Italiana Compliance

Regolamentazione e innovazione.
Compliance motore di sviluppo e sfida strategica
per la crescita aziendale

Indice

Prefazione

Claudio Cola
Presidente AICOM - Associazione Italiana Compliance

Compie venti anni il documento di Basilea "*Compliance and the compliance function in banks*"[1] che ha definito in ambito europeo il rischio di non conformità, ponendo a suo presidio la funzione di conformità (compliance), la stessa età di Aicom – Associazione Italiana Compliance.

Una corrispondenza temporale non casuale che evidenzia la costante presenza dell'associazione quale punto di riferimento dell'evoluzione della funzione di conformità, a partire dalla sua nascita e nella sua successiva importante crescita.

L'intervento di *soft-law* del Comitato di Basilea ha introdotto la funzione di compliance nelle banche e agevolato la sua successiva estensione alle aree dei servizi d'investimento e alle imprese d'assicurazioni così da ricomprenderle tra quelle che devono prevedere la presenza di tale funzione[2].

Una funzione a prevenzione del rischio di non conformità alle norme, a tutela della trasparenza e della correttezza dei comportamenti e all'affermazione ed alla diffusione di una cultura aziendale del rispetto delle regole di etero e auto regolamentazione all'interno delle organizzazioni complesse.

Sin dalla sua costituzione, l'Aicom ha inteso assicurare lo sviluppo della funzione, caratterizzata nei primi anni da un'attenzione prevalentemente rivolta a definirne ruoli e compiti, per poi orientarsi sempre più negli anni successivi verso una compliance dedicata ad ambiti normativi specialistici.

A partire dalla tutela del cliente, della reputazione, dei principi etici, la compliance acquista quindi negli anni una dimensione nuova, attenta ad aree caratterizzate da contenuti specialistici ad accentuata complessità tecnico-operativa (compliance IT, fiscale, antiriciclaggio, ecc.).

---

[1] Basel Committee on banking supervision, Compliance and the compliance function in banks (April 2005)

[2] Banca d'Italia, Disposizioni di vigilanza: la funzione di conformità (compliance) 10 luglio 2007; Regolamento Banca d'Italia e Consob del 29 ottobre 2007; ISVAPP, Regolamento del 26 marzo 2008.

D'altra parte, gli ambiti normativi di etero regolamentazione ricompresi nel perimetro della compliance nel tempo sono stati estesi sostanzialmente a tutte le normative applicabili alle aziende finanziaria, con la necessità di assicurare regole interne, processi e procedure a prevenzione della violazione delle norme stesse, dando sempre maggiore rilevanza alla funzione di compliance nell'assicurare assistenza e consulenza agli organi di vertice.

Una funzione quindi sempre più coinvolta nei processi decisionali e che, accanto alla sua originale garanzia di presidio del rispetto delle norme, può contribuire a creare valore aziendale e preservare la reputazione dell'azienda stessa che è alla base della fiducia prestata dalla clientela e più in generale dai numerosissimi *stakeholders* con i quali si relaziona.

Una funzione che diviene sempre più parte della governance bancaria quale presidio organizzativo e parte integrante e integrata del complessivo sistema dei controlli interni che si compone di un insieme di strutture, procedure e meccanismi volti ad assicurare che la gestione aziendale si attenga al pieno rispetto degli obiettivi di rischio approvati dall'organo di supervisione strategica[3].

In area finanziaria oramai è da considerarsi una presenza che contribuisce alla stabilità del sistema.

Inoltre, negli anni, anche grazie alla spinta associativa, la funzione allarga la sua area di riferimento all'industria e ai servizi non finanziari, per estendersi poi alla pubblica amministrazione.

Al riguardo una novità importante proviene dalle disposizioni UE in materia di antiriciclaggio ed in particolare dal Regolamento 2024/1624 che pone la funzione di conformità alle regole antiriciclaggio a tutela dell'integrità del sistema economico dai rischi di infiltrazione dei capitali illeciti.

Al riguardo il cd *Rule book AML* europeo prevede la nomina negli organi di gestione (in particolare per i soggetti finanziari) di un esponente responsabile della conformità (compliance manager) a prevenzione dei rischi di riciclaggio.

Sempre più, quindi, la compliance è funzione centrale e strategica nell'organizzazione aziendale in particolare delle realtà bancarie, assicurative e finanziarie in genere, attraverso una presenza proattiva nella prevenzione dei rischi di non conformità.

Una presenza che dialoga direttamente con il vertice aziendale e interagisce efficacemente con le altre funzioni aziendali sia di controllo e

[3] AICOM e AIIA, Le funzioni di internal Audit e di Compliance: ruoli, responsabilità e ambiti di rispettiva competenza, Milano, Aprile 2008.

sia di business, in posizione paritaria e con una centralità strategica a tutela della competitività e della crescita aziendale nel lungo periodo.

Una funzione che diviene sempre più strategica e destinataria di soluzioni tecnologiche che dovrà confrontarsi con una sempre più marcata dimensione specialistica degli ambiti normativi da presidiare, attraverso la definizione e il monitoraggio di procedure destinate ad assicurare la conformità dei comportamenti aziendali.

Una funzione le cui professionalità, vista la complessità normativa e tecnologica oramai parte essenziale degli sviluppi finanziari e non solo, devono assicurare una sempre maggiore interdisciplinarità e una formazione efficace che tenga conto di *skills* sempre più tecnologici con ricadute importanti in termini di formazione da dedicare sia ai collaboratori della funzione, da finalizzare in percorsi certificativi delle competenze affidabili ed efficaci, e sia a tutto il personale dell'azienda

Ciò a fronte dei nuovi rischi emergenti (*Cyber, cripto assets*, frodi digitali, ecc.) accanto a quelli tradizionali ma sempre più sofisticati (IT, AML, credito, ecc.) con una evoluzione di modelli operativi e distributivi complessi e che abbisognano di rigorosi standard di prevenzione.

Si pensi più in generale ai servizi finanziari la cui fornitura è assicurata tramite società terze, sia quali società fornitrici di servizi altamente tecnologici ai soggetti finanziari e sia, ultima tendenza, quali fornitori diretti dei servizi finanziari stessi.

Una situazione che evidenzia ed accompagna la rilevante ed attuale criticità delle politiche di esternalizzazione dei servizi bancari e finanziari e della stessa attività di compliance la cui corretta efficacia necessita di un forte governo dei fornitori terzi.

A questa centralità della funzione di conformità acquisita nelle due decadi della sua storia in Italia e più in generale in Europa, è stata dedicata l'iniziativa del 27 novembre 2025 presso il Dipartimento di Economia Aziendale dell'Università degli studi di Roma Tre dal titolo "L'evoluzione della funzione di compliance: da presidio al compliance risk a crescita strategica aziendale".

Un'iniziativa fortemente voluta dall'Aicom che si è potuta realizzare grazie alla collaborazione del Dipartimento di Economia aziendale dell'Università degli Studi di Roma Tre e del Compliance Lab nato negli scorsi anni ad opera del Dipartimento stesso e del quale l'Associazione è parte costitutiva.

Importanti relatori ai vertici delle istituzioni nazionali ed europee (Banca d'Italia, Consob, UIF, IVASS, EBA) si sono incontrati per confrontarsi, dai rispettivi angoli visuali, sulla evoluzione della funzione di confor-

mità e della sua sempre maggiore complessità organizzativa e di contenuti.

Le riflessioni espresse nei diversi ambiti di competenza della funzione di conformità, dall'area bancaria a quella finanziaria per arrivare a quella assicurativa, con attenzione altresì all'importante tema delle esternalizzazioni, confermano e rafforzano la natura strategica della funzione.

Un importante momento di riflessione tra le istituzioni di vigilanza e gli operatori professionisti della compliance e delle aree che interagiscono con essa; una sorta di nuovo punto di partenza della funzione stessa che, valutati i risultati raggiunti, consenta di tracciare le principali sfide presenti e future.

Pervenire ad una pubblicazione che raccolga i contributi ricevuti nella giornata di confronto è il naturale e, ci auguriamo, utile approdo di conoscenza per tutti coloro che professionalmente, ma anche in qualità di studiosi, si confrontano con la complessità di questa funzione.

La sequenza degli interventi e le considerazioni svolte nella tavola rotonda con gli importanti esponenti di primarie realtà finanziarie, consente di disporre di un insieme di concreti contributi operativi e spunti operativi particolarmente utili.

Una nuova stagione e nuove sfide che Aicom raccoglie con la sua presenza oramai ventennale.

I venti anni della funzione compliance

Claudio Clemente
Già Direttore dell'UIF - Unità di Informazione Finanziaria per l'Italia e Presidente Onorario AICOM – Associazione Italiana Compliance

1. Il Comitato di Basilea

Sono trascorsi ormai venti anni dal documento "*Compliance and the compliance function in banks*" pubblicato dal Comitato di Basilea per la vigilanza bancaria nell'aprile del 2005 sul rischio di conformità, definito come il rischio di sanzioni, significative perdite finanziarie o danni reputazionali derivanti dal mancato rispetto di norme, regolamenti, standards interni e codici di condotta.

Per fronteggiare tale rischio il documento sottolinea l'esigenza che le banche si dotino di una apposita funzione, complementare a quella di gestione degli altri rischi, ponendo in capo ai vertici aziendali la responsabilità della sua istituzione, supervisione e valutazione di adeguatezza e sottolineando come una cultura aziendale che enfatizzi l'onestà e l'integrità della condotta a partire dal vertice aziendale sia un importante presupposto per il rispetto delle regole.

Nel disegnare il perimetro della disciplina erano segnalate, in particolare, le prescrizioni relative ai rapporti con il mercato e con la clientela (condotta di mercato, trattamento dei clienti, adeguatezza della consulenza) e venivano incluse anche aree normative specifiche (quali le regole di prevenzione del riciclaggio e quelle fiscali rilevanti nella strutturazione dei prodotti) e sottolineati i rischi connessi ad ambiti operativi che possono consentire o facilitare condotte irregolari o illecite della clientela.

Sotto il profilo organizzativo era lasciata alle aziende la scelta della collocazione della funzione in relazione alle dimensioni e all'operatività (personale addetto presso le linee operative o presso un'unica struttura) considerando anche la possibilità di unità separate per aree specialistiche.

Indipendentemente dalla collocazione organizzativa, andavano assicurati alla funzione requisiti di indipendenza, adeguatezza delle risorse, chiarezza delle responsabilità attribuite e veniva previsto un periodico riesame della funzione ad opera dell'Internal Audit.

L'istituzione della nuova funzione si proponeva di evitare i rischi

di non conformità favorendo comportamenti coerenti con l'obiettivo del rispetto delle regole da parte dell'intera struttura operativa, attraverso la valutazione e la verifica dell'adeguatezza dei processi e delle procedure interne e con l'affermazione e la diffusione di una cultura aziendale che condizioni i comportamenti individuali del personale. Come sottolineato nel documento del Comitato di Basilea la conformità dovrebbe far parte della cultura dell'organizzazione e non solo del personale specializzato.

L'azione è quindi a carattere preventivo sui processi – assicurando la loro efficacia nell'evitare la violazione delle norme e verificandone successivamente l'adeguatezza – e sulla creazione e il mantenimento di valori aziendali incentrati sulla piena consapevolezza dell'esigenza del rispetto delle regole e dei rischi che derivano dalla loro violazione.

La previsione della nuova funzione ha richiesto una revisione dell'architettura del sistema dei controlli interni. Da un sistema che conferiva all'Internal Audit (o all'ispettorato interno) l'accertamento ex post dei comportamenti irregolari delle strutture operative responsabili del rispetto delle norme, si passava ad un sistema diretto a prevenire comportamenti non rispettosi delle regole operando sulla formazione del personale, sulla definizione dei processi operativi e sull'organizzazione assicurandone la coerenza con l'osservanza delle norme[4].

Veniva ad essere modificato l'obiettivo dell'attività di verifica: dall'individuazione delle anomalie con finalità essenzialmente repressive a quello, a più elevato valore aggiunto, volto ad evitare le violazioni attraverso la definizione e il monitoraggio delle procedure destinate a garantire comportamenti conformi, intervenendo con eventuali correttivi in caso di loro inadeguatezza.

2. Le disposizioni della Autorità nazionali

Al documento del Comitato di Basilea che invitava le autorità di vigilanza a verificare l'adozione da parte degli intermediari di idonei presidi al rischio di conformità, ha fatto seguito nel luglio del 2007 l'emanazione da parte della Banca d'Italia della prima disciplina della compliance in Italia[5] e nell'ottobre dello stesso anno del Regolamento congiunto della Banca

[4] S. De Polis, La funzione di *compliance* e l'antiriciclaggio nelle compagnie di assicurazione, intervento alla Tavola rotonda *Institute for Research of Law Economical and Social Studies* (I.R.L.E.S.S.), 18 novembre 2020.

[5] Banca d'Italia, Disposizioni di vigilanza, La funzione di conformità, del 10 luglio 2007.

d'Italia e della Consob con una analoga previsione riferita agli obblighi previsti dalle direttive europee in materia di correttezza e trasparenza nello svolgimento dei servizi e attività di investimento[6]. Nel marzo del 2008 anche l'Isvap chiedeva alle imprese di assicurazione l'istituzione della funzione di compliance nell'ambito della regolamentazione del sistema dei controlli interni delle imprese di assicurazione, disciplinandone caratteristiche e requisiti[7].

Le disposizioni delle autorità riprendevano le indicazioni del Comitato di Basilea come risposta alla crescente complessità del contesto esterno e dei relativi rischi e all'affermarsi di nuove sensibilità che richiedevano l'emanazione di regolamentazioni più articolate e in continuo aggiornamento, destinate a tutelare interessi pubblici di varia natura il cui mancato rispetto esponeva le aziende e in particolare quelle finanziarie alla possibilità di incorrere in sanzioni legali o amministrative e a danni reputazionali.

Nell'introdurre la nuova disciplina veniva osservato dalla Banca d'Italia come "Il rispetto delle norme e la correttezza negli affari costituiscono elementi fondamentali nello svolgimento dell'attività bancaria, che per sua natura è fondata sulla fiducia" e come l'evoluzione dei mercati finanziari rende più "complessi l'identificazione e il controllo dei comportamenti che possono dar luogo a violazioni delle norme, di standard operativi, di principi deontologici ed etici dell'attività di intermediazione" e richiede "da un lato, promuovere una cultura aziendale improntata a principi di onestà, correttezza e rispetto non solo della lettera, ma anche dello spirito, delle norme; dall'altro, approntare specifici presidi organizzativi, volti ad assicurare il rigoroso rispetto delle prescrizioni normative e di autoregolamentazione" con la istituzione, sulla base di criteri di proporzionalità, di una apposita funzione di prevenzione e gestione del rischio di violazione delle prescrizioni.

Erano, in proposito, richiamate le aree più rilevanti ai fini del presidio dei rischi di non conformità individuate in quelle riguardanti l'esercizio dell'attività di intermediazione, la gestione dei conflitti di interesse, la disciplina di trasparenza e di tutela del consumatore

Veniva precisato che la funzione deve individuare nel continuo le norme di eteroregolamentazione e di autoregolamentazione applicabili alla

[6] Regolamento della Banca d'Italia e della Consob del 29 ottobre 2007, art.16; Direttiva 2004/39/CE; Direttiva 2006/73/CE, art. 6; G. Carosio, La funzione di compliance tra Basilea II e MIFID, intervento al *III incontro Compliance AICOM*, 21 settembre 2007.

[7] ISVAP, Regolamento n. 20 del 26 marzo 2008, art 23.

banca, assicurare che le procedure interne siano in grado di prevenirne le violazioni, verificare la loro efficacia proponendo eventuali modifiche e predisporre adeguati flussi informativi per gli organi aziendali. La funzione deve anche valutare in via preventiva i rischi collegati ai progetti innovativi e l'adeguatezza della loro regolamentazione. Rientrano nei compiti della compliance l'assistenza e la consulenza agli organi di vertice e la collaborazione alla formazione del personale della banca in materia di conformità al fine di diffondere i principi di onestà, correttezza e di rispetto delle norme.

La rilevanza della nuova funzione era sottolineata dalle disposizioni di vigilanza che ne richiedevano, in linea con le indicazioni del Comitato di Basilea, l'adeguatezza qualitativa e quantitativa delle risorse e l'indipendenza attraverso la formalizzazione del mandato, l'autorevolezza, la professionalità e la congruità del ruolo del responsabile della funzione, la cui nomina e revoca erano attribuite al consiglio di amministrazione (o al consiglio di gestione) sentito il collegio sindacale e comunicate tempestivamente alla Banca d'Italia, adempimento quest'ultimo a ulteriore supporto dell'indipendenza dell'attività di verifica della conformità.

Veniva consentito l'accesso della funzione a tutte le informazioni ritenute rilevanti e la sua separazione dalla struttura di revisione interna, chiamata a verificarne periodicamente l'azione.

3. Gli sviluppi della funzione di compliance

Nel corso degli anni la funzione è stata interessata da interventi regolamentari e indicazioni da parte delle autorità.

Nell'ambito di una riformulazione complessiva delle disposizioni relative al sistema dei controlli interni delle banche, è stata più chiaramente definita la collocazione organizzativa della funzione di compliance indicando anche le sue relazioni con le altre funzioni aziendali di controllo dei rischi e di revisione interna. Ne venivano meglio indicati il perimetro operativo, secondo un approccio basato sul rischio, e i compiti attribuiti, con lo svolgimento di un ruolo sempre più trasversale in collegamento con le altre strutture di presidio specialistico per la definizione delle relative procedure e delle metodologie di valutazione dei rischi di non conformità. Alla funzione era anche attribuito il compito di verificare la coerenza del sistema premiante con il rispetto delle norme, codici etici, standard di condotta[8].

È stata ulteriormente valorizzata la funzione di conformità nel si-

[8] Banca d'Italia, Circolare n. 285 del 17 dicembre 2013 e successivi aggiornamenti.

stema di governo degli operatori dei mercati finanziari, in particolare, nella valutazione della governance dei prodotti e sono stati ulteriormente precisati i requisiti soggettivi degli addetti alla funzione e del suo responsabile che dovrebbe, tra l'altro, possedere esperienza ed essere dotato di elevati principi etici, professionali e di integrità personale[9].

Gli sviluppi della regolamentazione hanno accompagnato e stimolato l'evoluzione della funzione in questi anni.

L'attività di prevenzione dei rischi di non conformità tende a realizzarsi, oltre che mediante la verifica dell'adeguatezza delle procedure, anche attraverso la valutazione degli impatti normativi connessi con le decisioni strategiche, in particolare mediante l'analisi dei nuovi progetti aziendali e dei processi ad essi collegati[10]. La funzione di compliance è così chiamata a svolgere un'attività di consulenza e di supporto degli organi di governo anche nella definizione delle prospettive aziendali, assistendoli nella valutazione dei rischi legali e reputazionali derivanti da tali decisioni[11].

Le conoscenze aggiornate delle diverse normative alle quali i soggetti finanziari sono sottoposti consentono di aumentare la consapevolezza dei rischi della gestione e di contribuire alla valutazione della convenienza delle strategie e dell'opportunità di nuovi investimenti.

Il coinvolgimento della funzione di compliance nella identificazione degli impatti delle decisioni strategiche in termini di rischi di non conformità contribuisce ad orientare le scelte verso prospettive operative sostenibili nel lungo termine, proteggendo le aziende dai costi delle violazioni e soprattutto preservandone reputazione e affidabilità.

Il contributo della compliance alla pianificazione strategica rende possibile una più elevata capacità degli organi aziendali di assumere decisioni consapevoli e di adattarsi con maggiore rapidità ai mutamenti normativi con conseguenti vantaggi competitivi.

L'introduzione di nuovi prodotti non può prescindere anche dalla valutazione dei rischi legali e reputazionali che occorre affrontare e che debbono orientare le decisioni ma che possono essere mitigati attraverso presidi procedurali e organizzativi.

---

[9] Comunicazione congiunta Banca d'Italia-Consob dell'8 marzo 2011; Direttiva 2014/65/UE; ESMA, Orientamenti su alcuni aspetti dei requisiti della MIFID II relativi alla funzione di controllo della conformità, 6 aprile 2021.

[10] G. Boccuzzi, Prefazione, P. Murè, Manuale Compliance, EGEA, luglio 2025.

[11] Con la comunicazione congiunta Banca d'Italia-Consob del 2011 (cfr. nota 6) nel precisare meglio il ruolo della funzione di conformità nell'organizzazione aziendale si sottolineava che la compliance valuta il rischio di non conformità sotteso alle scelte strategiche.

Ignorare o, all'opposto, enfatizzare tali rischi comporta riflessi sul piano economico esponendo l'azienda alle conseguenze del mancato rispetto delle norme ovvero della perdita di opportunità di mercato, in entrambi i casi con impatti sulla sua immagine.

La scelta di rinunciare a taluni prodotti o a fasce di clientela in relazione ai pur gestibili rischi legali ad essi connessi è sicuramente comprensibile ma evitabile, anche nell'ottica di favorire l'inclusione finanziaria, con l'ausilio di una efficiente funzione di compliance.

4. La compliance antiriciclaggio

Alla continua evoluzione della disciplina antiriciclaggio va fatta risalire la spinta verso lo sviluppo di specifiche regole in materia di conformità per un comparto regolamentare a forte connotazione specialistica.[12]

Nel documento di Basilea del 2005 tale normativa veniva richiamata esplicitamente tra quelle rientranti nel perimetro della funzione di compliance ma appartenenti ad aree con caratteristiche peculiari, come la materia fiscale, che richiedono competenze specifiche.

Le crescenti esigenze di contrasto al riciclaggio e, successivamente, al finanziamento del terrorismo assieme alla complessità della disciplina di prevenzione richiedono elevati presidi interni che, considerata la peculiarità delle finalità della disciplina, non possono, a maggior ragione, limitarsi alla verifica di aspetti formali, specie con riguardo al rispetto degli obblighi di collaborazione attiva, richiedendo anche un più esteso ricorso all'ausilio di strumenti e soluzioni tecnologiche anche avanzate.

L'evoluzione più recente della regolamentazione secondaria in materia di antiriciclaggio ha portato, tra l'altro, alla previsione per gli operatori finanziari[13] di un componente dell'organo amministrativo quale esponente responsabile per l'antiriciclaggio, principale punto di contatto tra il titolare

[12] Banca d'Italia, Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo, 26 marzo 2019; IVASS, Regolamento n.44 del 12 febbraio 2019 in materia di organizzazione, procedure, controlli interni; CONSOB, Regolamento n. 20570 del 4 settembre 2018 di attuazione del d.lgs. 231/2007 per i revisori legali.

[13] Banca d'Italia, Provvedimento del 1° agosto 2023 di modifica delle Disposizioni in materia di organizzazione, procedure e controlli interni per finalità antiriciclaggio del 26 marzo 2019; IVASS, Provvedimento n. 144 del 4 giugno 2024 che modifica il Regolamento IVASS n. 44 del 2019.

della specifica funzione di prevenzione e gli organi aziendali. La previsione della nuova figura è stata confermata dal recente Regolamento europeo AML/CFT[14] che, nel disciplinare in maniera dettagliata "la funzione di controllo della conformità antiriciclaggio" e l'attività del suo titolare, porta a livello di regolamentazione europea l'obbligo di individuare un membro dell'organo di gestione (compliance manager) con il compito di garantire che siano rispettate le previsioni normative e amministrative di prevenzione del riciclaggio e che le politiche interne, le procedure e i controlli siano coerenti con l'esposizione al relativo rischio.

Con l'entrata in vigore della nuova disciplina europea (a partire da luglio 2027), la previsione di una funzione di conformità riferita alla normativa antiriciclaggio riguarderà tutti i soggetti obbligati e non solo quelli finanziari e coinvolgerà anche il rispetto degli obblighi relativi all'applicazione delle sanzioni finanziarie mirate. Si viene così a determinare un ampliamento delle regole da presidiare con la specifica funzione e una estensione della platea degli operatori tenuti ad istituirla che sono chiamati, pertanto, ad affrontare una rilevante sfida organizzativa.

5. La conformità non riguarda solo gli intermediari finanziari

L'esigenza di protezione dai rischi legali e reputazionali derivanti dal mancato rispetto delle norme prescinde da obblighi regolamentari ed è presente in tutte le strutture organizzative e quindi sia nelle imprese diverse da quelle finanziarie sia nelle pubbliche amministrazioni.

Come è emerso dalla survey promossa da AICOM e Protiviti[15], una parte assolutamente preponderante delle imprese che hanno partecipato alla rilevazione (circa 70 aziende per più della metà quotate) si è dotata di una funzione di conformità chiamata a fronteggiare il rispetto di normative eterogenee e sempre più articolate, ricorrendo, tuttavia, a soluzioni che, a differenza delle imprese vigilate, non seguono un disegno omogeneo nell'architettura della funzione, mancando una disciplina di riferimento.

Pure il settore pubblico ha manifestato nel tempo qualche interesse alle logiche della compliance basate su modalità di controllo preventivo a carattere non burocratico[16]. Inizialmente sono state, in particolare, le pro-

[14] Regolamento (UE) 2024/1624, art. 11 - Funzione di controllo della conformità.

[15] AICOM - Protiviti, Compliance Governance. Presente e futuro nel settore manufatturiero e dei servizi non finanziari, maggio 2025

[16] AA.VV. La compliance nella Pubblica Amministrazione, Bancaria Editrice, maggio 2013.

cedure degli appalti ad essere oggetto di attenzione, in considerazione della complessità delle relative regole e della loro diffusa applicazione nel comparto pubblico. Successivamente, le modifiche intervenute nelle norme antiriciclaggio per gli uffici della Pubblica Amministrazione e la conseguente emanazione di specifiche indicazioni organizzative hanno sollecitato nuovo interesse alla materia dei controlli di conformità, pur determinando un approccio concreto da parte di un numero contenuto di strutture.

6. Conclusioni

La crescente complessità del quadro normativo di riferimento delle aziende – sempre più dettagliato, articolato e in costante evoluzione per fronteggiare anche nuove finalità – assieme alla più elevata attenzione al rispetto di principi di correttezza hanno dato maggior rilievo al ruolo della funzione di compliance e ne hanno accresciuto in maniera significativa le responsabilità con riguardo sia all'ampiezza dell'area di competenza sia alle esigenze di collegamento con le altre attività di controllo.

La funzione è chiamata a contribuire al governo dell'azienda attraverso il presidio del rischio di conformità con un approccio proattivo integrato nelle logiche operative e di governance e realizzato mediante l'analisi dei processi, l'apporto alla creazione di una cultura aziendale ispirata alla legalità e all'etica, il coinvolgimento nella valutazione dei rischi connessi alle strategie.

La previsione della funzione di compliance e la sua regolamentazione contenuta nelle diverse disposizioni delle autorità risponde a finalità pubbliche ma realizza anche obiettivi di natura privata.

Sotto quest'ultimo profilo, un efficace svolgimento della funzione contribuisce a mantenere e accrescere il valore aziendale (compliance come mezzo di creazione di valore) collaborando a garantire i risultati futuri attraverso il presidio sia dei rischi economici derivanti dalla mancata osservanza del complesso delle norme a cui l'azienda è assoggettata, sia dei rischi connessi alla perdita della fiducia della clientela, degli investitori e del mercato, patrimonio fondamentale, in particolare, per un intermediario finanziario.

La funzione di conformità e il suo rafforzamento costituisce, pertanto, una scelta strategica che può consentire all'azienda di preservare e migliorare la propria reputazione e assicurare un adeguato supporto agli organi amministrativi nelle valutazioni delle prospettive aziendali, elementi che assumono rilevante importanza per il raggiungimento in sicurezza degli obiettivi di impresa nel lungo periodo.

Sotto il profilo delle finalità pubbliche sottese alle disposizioni di vigilanza che si collegano, in particolare, alla tutela degli interessi della clientela e alla stabilità del sistema, la previsione nel Regolamento europeo AML/CFT di una specifica disciplina della funzione di conformità alle regole antiriciclaggio rappresenta un ulteriore conferma dell'importanza attribuita alla compliance con riferimento, in questo caso, al rispetto di una disciplina finalizzata a preservare l'integrità del sistema economico nazionale e internazionale dai rischi di infiltrazione di capitali illeciti. A tale rilevante finalità sembra possa essere fatta risalire la peculiare previsione, ai fini del rispetto delle disposizioni antiriciclaggio, dell'esponente responsabile della conformità (il compliance manager), ora assurta a rango regolamentare ed estesa a tutti i soggetti obbligati.

L'attività di compliance. Evoluzione della funzione e appunti di vigilanza

Giuseppe Siani
Capo del Dipartimento Vigilanza bancaria e finanziaria della Banca d'Italia

1. Introduzione

In un contesto di forti cambiamenti e innovazione, aumentano ampiezza e complessità dei compiti affidati alla funzione di conformità e si aggiornano le aspettative della Vigilanza. In generale, comunque, la Compliance, oltre ad assicurare nel continuo un presidio a fronte del complessivo profilo di rischio, deve favorire la diffusione all'interno dell'azienda di una cultura attenta ai rischi, in cui sia riconosciuta centralità anche ai profili di conformità alle norme e alla relazione con la clientela.

Dopo aver ripercorso l'evoluzione di questa funzione di controllo, vorrei condividere esperienze operative di vigilanza che possono aiutare a identificare alcuni fattori chiave per garantirne il necessario ruolo strategico.

2. Evoluzione della funzione

La centralità della funzione di conformità nell'organizzazione degli intermediari bancari e finanziari non è solo legata alla più recente evoluzione dei rischi e dell'operatività aziendale, ma è anche il riflesso di un quadro normativo internazionale e nazionale che si è consolidato nel corso degli anni, che ne definisce il ruolo, la collocazione organizzativa e la relativa attività nell'ambito del sistema dei controlli interni.

Nel tempo, requisiti e presidi normativi sono stati rafforzati, prevedendo un maggiore coinvolgimento della Compliance nei processi aziendali e un rafforzamento della sua indipendenza – anche nei confronti delle altre funzioni di controllo, oltre che di quelle commerciali e operative – e del coordinamento con gli organi aziendali[17].

[17] Si vedano ad esempio i *Core Principles for Effective Banking Supervision* del Comitato di Basilea sulla supervisione Bancaria, le *Guidelines on Internal Governance* dell'EBA e, a livello na-

Ampiezza e articolazione dei compiti della funzione di conformità sono aumentati progressivamente, in linea con la crescente complessità operativa e normativa che caratterizza il settore. Ad esempio, la profonda trasformazione digitale che sta interessando banche e intermediari finanziari si riflette in una rapida innovazione dei processi e dei prodotti e servizi offerti alla clientela, facendo emergere rischi nuovi (cyber, ESG, frodi digitali, rischi di natura globale dei *cripto-assets* anche connessi alla "pseudo anonimità" delle transazioni) e aumentando l'intensità di alcuni rischi più tradizionali (IT, terze parti, AML, credito).

Questa evoluzione di modelli operativi e strategie è accompagnata da quella delle norme di riferimento: sono infatti entrati in vigore standard tecnici più rigorosi e dettagliati (Regolamento DORA, MiCAR e AI Act) che impongono nuovi compiti alle Autorità e agli enti vigilati e, di conseguenza, rilevanti investimenti, anche in termini di competenze. In questo quadro è necessario che le funzioni di controllo (i) aggiornino ed estendano le proprie conoscenze specialistiche, (ii) adottino una visione ampia dei processi e un approccio interdisciplinare e integrato, e (iii) possano contare su una solida governance dei dati.

Per la funzione di conformità – chiamata insieme al risk management a gestire il rischio collegato con la tecnologia – gli impatti sono chiaramente significativi e ne vorrei commentare in particolare due: il rafforzamento della valenza strategica del suo ruolo, a supporto degli organi aziendali; il potenziale impiego di tecnologie avanzate per potenziare i controlli.

Per quanto riguarda il primo aspetto, la Compliance deve definitivamente superare approcci di tipo reattivo/correttivo; è fondamentale che sia sistematicamente coinvolta nei processi decisionali, per svolgere valutazioni preventive sulle iniziative innovative e, ove opportuno, consentire di orientare o ricalibrare le scelte in modo da preservare la resilienza del modello operativo. Ad esempio, l'ingresso in nuovi comparti di attività, la modifica di processi o di applicativi di supporto, la revisione delle politiche distributive, sono progetti in cui è fondamentale individuare fin dalla fase iniziale i potenziali rischi di non conformità da presidiare, non solo per attuare scelte strategiche sostenibili, ma anche per minimizzare il rischio di costosi interventi correttivi *ex post*. In questo modo, la funzione di conformità non solo assicura il perseguimento degli obiettivi sottesi alle norme di cui garantisce il rispetto, ma contribuisce anche a creare valore per

zionale, da ultimo le Disposizioni della Banca d'Italia relative ai mercati delle criptoattività del 1° ottobre 2025.

l'azienda e a preservare il rapporto fiduciario con la clientela.

Questo ruolo maggiormente strategico è richiesto anche a fronte dei rischi di riciclaggio e finanziamento del terrorismo (AML), tenuto conto che le nuove norme prevedono che venga individuato un referente AML tra i membri del *board* e che la gestione di questa tipologia di rischi sia affidata a una funzione di controllo dedicata[18].

Il coinvolgimento preventivo della funzione di compliance è un elemento essenziale anche nei processi di *product governance*; in particolare, la disciplina di tutela impone agli intermediari di adottare procedure di governo e controllo (c.d. disciplina POG – *Product Oversight and Governance*) che, sin dalla fase di ideazione del prodotto e per tutto il ciclo di vita, tengano in considerazione gli interessi, gli obiettivi e le caratteristiche dei clienti, per garantire presidi sostanziali dei rischi.

Al disegno di processi decisionali che prevedano valutazioni *ex ante* di compliance, deve però accompagnarsi un approccio proattivo da parte della stessa funzione di conformità, sia all'interno – per sensibilizzare gli organi di vertice, le altre funzioni di controllo e quelle di business sui profili di conformità rilevanti di ogni scelta aziendale – sia verso l'Autorità di vigilanza, in veste di interlocutore qualificato, che anticipa la gestione di potenziali criticità.

Con riferimento al secondo aspetto, l'impiego delle tecnologie più avanzate nel business bancario impone alla Compliance un ampliamento e una revisione della propria missione, ma, in prospettiva, può anche assicurare un valido supporto per agevolarne il compito e rafforzarne l'efficacia.

Nella nostra esperienza di supervisione osserviamo prime soluzioni innovative, quali ad esempio l'utilizzo di assistenti di intelligenza artificiale (AI) a supporto delle attività di controllo, che permette in via automatica la raccolta di informazioni, la classificazione dei flussi di reporting di altre funzioni, l'analisi di rischio attraverso esami incrociati di documenti (interni ed esterni). Anche le verifiche in materia di antiriciclaggio rappresentano un "laboratorio" in cui vengono sviluppate e sperimentate nuove tecnologie, in particolare per l'acquisizione e il controllo della clientela. In proposito, segnalo gli esiti di una recente indagine[19] che ha rilevato come scelte

[18] Si vedano le Disposizioni della Banca d'Italia in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari ai fini di riciclaggio e di finanziamento del terrorismo del 26 marzo 2019, così come modificate dal Provvedimento del 1° agosto 2023.

[19] "Indagine qualitativa sull'adozione di strumenti innovativi per l'assolvimento degli obblighi AML/CFT" pubblicata il 2 settembre 2025. Gli esiti dell'indagine sono stati anche

tecnologiche innovative per l'adempimento degli obblighi antiriciclaggio possano effettivamente accrescere l'efficienza e l'efficacia dei presidi.

L'impiego di strumenti di AI può aiutare a fronteggiare la complessità e anche favorire l'*accountability* e la diffusione di una cultura organizzativa orientata alla conformità, ad esempio perché può consentire di strutturare indicatori che facilitino il confronto interno su criticità e azioni correttive, stimolino comportamenti conformi, contribuiscano a dare piena visibilità alle attività della Compliance e renderne misurabile l'operato.

L'aggiornamento in questa direzione degli strumenti e dei processi di controllo è ancora in una fase iniziale nel settore. Mostra certamente potenzialità elevate, anche in una logica di contenimento dei costi, ma pone anche nuovi rischi (*bias*, *privacy*, trasparenza) che vanno censiti e governati nel contesto di una più ampia strategia di trasformazione digitale dei controlli; richiede alle funzioni preposte nuove competenze, flessibilità e capacità di adattamento. L'utilizzo di strumenti basati sulle tecnologie più avanzate non deve in nessun caso far venir meno la responsabilità delle funzioni e il coinvolgimento della componente umana nei processi decisionali; deve inserirsi in un percorso di valutazione strutturato e robusto, accompagnato da articolati programmi di preparazione e formazione delle risorse.

3. Appunti di vigilanza

La Banca d'Italia presta massima attenzione alla qualità dei presidi di controllo, elemento cruciale dell'organizzazione aziendale per garantire la resilienza dei singoli intermediari e del sistema nel suo complesso.

L'efficacia della Compliance viene valutata (dalle funzioni di Vigilanza – anche in coordinamento con la Banca Centrale Europea per le banche 'significative' – Antiriciclaggio e di Tutela della Banca d'Italia) nel corso dell'ordinaria attività di supervisione, attivando un'ampia gamma di strumenti, quali ad esempio gli incontri con le funzioni di controllo e il management, l'analisi a distanza, le ispezioni, le analisi di confronto orizzontale e di sistema. La Banca d'Italia favorisce, inoltre, il continuo dialogo con l'industria per chiarire le aspettative della Vigilanza e acquisire contributi dagli intermediari.

Vorrei oggi condividere brevemente alcuni risultati dell'esperienza operativa maturata finora. In primo luogo, la situazione è alquanto etero-

presentati in un workshop organizzato dalla Banca d'Italia lo scorso 4 novembre.

genea con "luci e ombre" sul ruolo e l'efficacia della funzione di conformità; in molti casi esaminati dalla Vigilanza è ancora lungo il percorso verso una funzione realmente strategica, multidisciplinare e ben integrata nel complessivo sistema di governo aziendale. Per alcuni operatori, infatti, si deve ancora realizzare un cambio di paradigma operativo tale da superare la percezione della Compliance come mero centro di costo; il tema riguarda in modo particolare le banche e gli intermediari di dimensioni più piccole, che devono trovare un complesso equilibrio tra obiettivi di efficacia e risparmio dei costi.

Le nostre evidenze mostrano, inoltre, che la funzione non svolge sempre il proprio ruolo in maniera pervasiva; registriamo lacune nel perimetro di indagine, inadeguato livello di approfondimento delle analisi e scarsa efficacia delle attività di *follow up*. Mi vorrei soffermare in particolare su tre ambiti principali in cui ne possono essere ricercate le cause: i) assetti organizzativi e quindi anche di esternalizzazione, ii) gestione integrata dei rischi e iii) dotazione di risorse.

Per gli operatori più piccoli, l'accesso a risorse più ampie e scalabili e a competenze specialistiche qualificate, a costi sostenibili, viene spesso ricercato affidando a fornitori esterni alcune attività di controllo. Le analisi della Banca d'Italia evidenziano peraltro che quando le attività di conformità vengono esternalizzate, la loro efficacia dipende in larga misura dalla presenza di un governo forte e attento dell'attività dei fornitori. Se il controllo è debole, manca un'adeguata strategia di gestione dell'attività esternalizzata, anche un contratto ben fatto non basta.

Abbiamo visto casi in cui le attività di compliance perdono efficacia perché il fornitore presta all'intermediario anche servizi di tipo operativo e si trova quindi in una situazione di potenziale conflitto di interesse. Presso altri intermediari il presidio è risultato fragile perché sono state accettate "passivamente" le soluzioni standard proposte dal fornitore, magari poco costose ma non adatte alle specificità del business; in queste situazioni, in sostanza, manca una valutazione degli specifici rischi di non conformità connessi con l'operatività aziendale, la pianificazione della funzione non risulta, quindi, improntata a una logica *risk based* e gli oggetti delle indagini da svolgere, definiti in modo generico, non colgono i peculiari tratti operativi dell'intermediario.

Attivare un sistema robusto di monitoraggio delle attività affidate in outsourcing deve essere tra le priorità dell'azienda perché – come ho già avuto modo di richiamare in un recente intervento a Torino – esternalizzare non significa per un intermediario liberarsi della responsabilità perché questa rimane in capo agli organi aziendali.

Parlando ancora di assetti organizzativi e operativi, una soluzione alternativa che riscontriamo presso operatori di minori dimensioni, sempre in una logica di contenimento dei costi, è quella di fondere le attività di controllo di secondo livello in una funzione unica, tipicamente incaricata di attività di conformità, di antiriciclaggio e di risk management. Si tratta di una decisione che merita un'attenta valutazione, che non deve essere guidata solo dalla dimensione aziendale, come abbiamo osservato in alcuni casi. Il concetto di proporzionalità – la normativa lo chiarisce – non può infatti prescindere da considerazioni più mirate sulla complessità del modello operativo e sulla entità e la natura dei rischi assunti.

Il secondo tema che mi sta a cuore riguarda l'importanza della visione integrata dei rischi, un altro elemento essenziale per consentire all'organo amministrativo aziendale di assumere decisioni sostenibili. Nella nostra attività di supervisione riscontriamo anche casi di forte indebolimento dei presidi per un carente coordinamento della Compliance con le altre funzioni di controllo: quando manca un'interazione strutturata e continuativa, a volte anche in presenza di una ripartizione di compiti e responsabilità non chiara, abbiamo osservato sovrapposizioni e lacune che minano l'efficienza e l'efficacia dei controlli. L'esigenza di questo raccordo è particolarmente evidente oggi, vista la crescente interconnessione tra diverse tipologie di rischio (di credito, operativi, di riciclaggio, cyber, ESG). Ad esempio, un intermediario vigilato ha sottostimato il rischio di un business innovativo, perché le valutazioni si sono concentrate sul tradizionale rischio di credito e non sono state integrate da un'analisi adeguata del connesso rischio di riciclaggio, che si è rivelato di dimensione tale da mettere potenzialmente in discussione l'effettiva sostenibilità del modello operativo.

Quando parlo di visione integrata dei rischi non mi riferisco, però, solo ai tempi e alle modalità di interazione tra i responsabili dei controlli o alla qualità del reporting destinato agli organi di vertice. A monte, è necessario un *framework* di *data governance* robusto, che assicuri accessibilità, qualità, sicurezza e tracciabilità delle informazioni sui rischi che supportano le attività delle funzioni di controllo: su questo aspetto le nostre analisi evidenziano carenze, anche importanti in alcuni casi, che mettono in luce una generalizzata necessità di elevare il livello di attenzione da parte degli intermediari.

Un ruolo marginale e poco incisivo della funzione di conformità può però dipendere anche da un'insufficiente dotazione di risorse. È una criticità che emerge con una certa ricorrenza dalle nostre analisi; osserviamo che quando mancano competenze o supporti adeguati e coerenti con l'articolazione della missione affidata, la funzione non riesce a rispettale il

piano delle verifiche necessarie, a garantire controlli estesi a tutti gli ambiti rilevanti e sufficientemente approfonditi, non è in grado di assumere un ruolo strategico e rischia anche di perdere indipendenza. Questo succede, ad esempio, in contesti caratterizzati da carenze diffuse negli organici delle strutture aziendali, in cui le risorse assegnate alla funzione di conformità sono coinvolte anche in attività operative.

Vorrei ora concludere questa panoramica con una considerazione di natura strategica sull'esigenza di assicurare la presenza di una caratteristica aziendale che consente di mitigare e superare tutti gli elementi di fragilità e di attenzione che ho ricordato.

Faccio riferimento al ruolo attento e attivo del *board,* elemento presente in tutti i casi in cui la funzione fornisce un contributo davvero efficace per contenere i rischi e mantenere condizioni di stabilità dell'azienda. Il tono dato dal vertice è infatti importante per tre ordini di ragioni: 1) si traduce in investimenti e stimolo costante ad affinare le metodologie di controllo; 2) è fondamentale per promuovere un modello culturale che riconosca un valore strategico alla conformità alle norme e alla tutela del cliente; 3) una corretta sensibilità degli organi di vertice ai profili di conformità garantisce non solo l'integrazione delle relative valutazioni nei processi chiave e nelle scelte strategiche, ma anche l'attivazione di leve efficaci per orientare i comportamenti a tutti i livelli aziendali (formazione, *accountability*, incentivi).

Nell'esperienza della Vigilanza la funzione si dimostra ben strutturata ed efficace in contesti in cui gli organi aziendali riconoscono la valenza strategica del presidio di conformità e sono ingaggiati nel rivalutarne periodicamente la funzionalità e l'adeguamento, anche attraverso iniziative di digitalizzazione e automatizzazione dei processi.

In ambito AML, la nomina di un referente tra i membri del CdA – che, come ho prima richiamato, è stata imposta da un recente aggiornamento normativo – crea un collegamento più immediato tra l'organo di supervisione strategica e la funzione antiriciclaggio e rappresenta un forte impulso ai *board* a evolvere verso un approccio attento e attivo. Come abbiamo però osservato in alcuni casi, la sola nomina di un consigliere referente AML non basta: perché questo ulteriore presidio funzioni davvero e porti a interventi concreti per ridurre i rischi e migliorare i processi di controllo, è essenziale che l'esponente individuato abbia competenze adeguate, esperienza, sia proattivo e abbia tempo sufficiente da dedicare al ruolo.

4. Conclusioni

Vorrei concludere riprendendo tre concetti chiave di questa riflessione sulle sfide evolutive della funzione di conformità nel contesto attuale: ruolo strategico e proattivo, *tone from the top*, governo unitario.

La funzione di compliance si trova oggi di fronte a una sfida cruciale: dimostrare di essere non solo un presidio tecnico, ma un elemento abilitante della sostenibilità e della resilienza aziendale. In un ecosistema finanziario sempre più interconnesso, digitale e soggetto a pressioni normative e reputazionali, la conformità deve essere considerata non un vincolo, bensì una leva strategica per la competitività e la creazione di valore nel lungo periodo.

Per compiere questo salto di paradigma, è necessario che la Compliance superi una logica meramente formale e reattiva assumendo un ruolo proattivo nelle decisioni strategiche, capace di contribuire alla definizione delle priorità aziendali e alla costruzione di modelli operativi robusti e trasparenti. Questo può comportare la necessità di una profonda trasformazione culturale, che deve partire dai vertici aziendali per permeare l'intera organizzazione, promuovendo comportamenti coerenti, consapevolezza diffusa e una visione condivisa del valore della conformità.

In tale prospettiva, il futuro della Compliance sarà sempre più legato alla capacità di interpretare il cambiamento, fronteggiare la complessità, anticipare i rischi emergenti e presidiare le aree di innovazione con strumenti adeguati e competenze evolute. È cruciale mantenere e rafforzare un raccordo efficace con le altre funzioni di controllo per garantire una visione e una gestione integrata dei rischi. La tecnologia, se ben governata, può rappresentare un alleato prezioso, ma richiede un investimento continuo in formazione, analisi critica e adattamento dei modelli di controllo.

La crescente complessità del contesto operativo e normativo ha stimolato una articolazione sempre maggiore e la specializzazione dei presidi di conformità. Mantenere un forte governo unitario della funzione, è però necessario per garantire un'efficace integrazione delle attività di compliance nei processi decisionali strategici e nel più complessivo sistema di governo e controllo aziendale, oltre che per assicurare un raccordo efficace con tutti gli *stakeholders* interni ed esterni. La Banca d'Italia, che pure vigila attraverso diverse strutture, fa la sua parte perseguendo costantemente una valutazione integrata dell'adeguatezza dei presidi degli intermediari e garantendo un'azione di intervento sempre coordinata.

L'obiettivo comune deve essere quello di costruire un sistema di conformità in grado di coniugare rigore e flessibilità e di affrontare con

competenza e responsabilità le sfide del futuro, per contribuire concretamente alla resilienza del sistema finanziario e alla tutela degli interessi della clientela.

Innovazione tecnologica, tutela dei mercati e degli investitori; il ruolo della funzione di compliance nel presidio dei nuovi rischi

Andrea Turi
Responsabile della Divisione Vigilanza Intermediari e Protezione Investitori - Consob

1. Finanza e tecnologia

Finanza e tecnologia hanno da sempre avuto una relazione simbiotica. Se solo da qualche anno si parla più modernamente di fintech, crasi delle parole finanza e tecnologia, traducibile nella formulazione generica "tecnologia applicata alla finanza", questa fratellanza siamese fra le due aree rappresenta un trend secolare.

La finanza ha storicamente sospinto gli sviluppi tecnologici sin dalla rivoluzione industriale, mettendo a disposizione ingenti capitali nei secoli XVIII e XIX. Di converso, ed è quello che oggi ci occupa, per secoli il progresso tecnologico è stato una forza trainante ed evolutiva del settore finanziario, in accelerazione nei tempi più recenti.

La finanza si nutre infatti di informazioni e di analisi delle stesse e dunque incidono profondamente su di essa tutte le innovazioni che agevolano comunicazioni e trattamento dei dati; alla luce di questo, l'ultimo secolo, con i tumultuosi sviluppi della scienza dell'informazione e delle tecnologie digitali, è stato quindi particolarmente fecondo per questo rapporto.

Riguardando al recente passato, non si può non osservare come l'industria dei servizi finanziari sia stata tra i maggiori fruitori della rivoluzione informatica a livello globale.

Secondo taluni studiosi, la relazione tra finanza e tecnologia può essere scomposta in tre epoche, ciascuna contraddistinta da caratteristiche peculiari e specificità ben determinate.

La prima, connotata da soluzioni prettamente "analogiche" (ad esempio ATM, carte di credito, fax, telex) si protrae fino alle soglie degli anni 70 con l'introduzione del primo sportello bancario automatico da parte di Barclays. Da quel periodo si avvia una seconda fase caratterizzata dalla progressiva spinta alla digitalizzazione che si insinua in tutti i processi finanziari. Infine, dalle propaggini della grande crisi del 2008 nasce una terza fase, tuttora in corso, con una spinta alla telematizzazione che reca

con sé il fenomeno del mobile, dei big data, delle grandi piattaforme ibride.

Ci si riferisce, a titolo di esempio, al fenomeno delle cosiddette "superapp" che consentono di accedere ad una sempre più vasta gamma di servizi, anche di investimento; esse sono tipicamente realizzate e fornite prevalentemente da società tecnologiche, quindi da parte di soggetti di natura non finanziaria, portando dunque ad una crescente fluidità dei confini tra prestatori dei servizi e interfaccia per la prestazione degli stessi.

2. La Compliance nel nuovo contesto

Emerge in maniera sempre più evidente nel contesto attuale, come tali ultime innovazioni stiano incidendo, e ancor di più incideranno, in maniera talmente pervasiva sulle modalità di prestazione dei servizi d'investimento e sulle modalità di interazione con la clientela da porre sfide nuove e molto importanti anche per la Compliance che deve, da una parte assecondare lo sviluppo dei processi in una prospettiva di efficacia ed efficienza, ma anche verificare che tutte le attività siano effettivamente svolte nel modo più coerente con la disciplina.

Nel contesto storico che stiamo vivendo, l'adozione di un efficace presidio della conformità alle norme assume, ancor più, una rilevanza fondamentale nell'ambito del complessivo sistema dei controlli.

Il principio cardine dettato dalla disciplina per l'attività di intermediazione mobiliare è infatti quello della cura dell'interesse del cliente.

Se le altre funzioni del sistema dei controlli (Internal Audit, Risk Management) sono precipuamente rivolte, in prima battuta, alla tutela degli interessi dell'azienda, la Compliance tende a presidiare in via diretta ed immediata soprattutto l'interesse della clientela a mezzo della verifica del rispetto della ridetta disciplina.

Peraltro, il compito di assicurare la conformità dei comportamenti alle norme ha assunto negli ultimi anni connotati e configurazioni sempre diverse, in un contesto di progressivo sviluppo dell'industria dei servizi finanziari e di conseguente proliferazione di nuove attività, prodotti e modelli operativi.

Se alla sua introduzione, l'operato della Funzione di controllo di conformità alle norme si concentrava prevalentemente "a valle" con l'intento di "limitare i danni", eventualmente generati da una attività commerciale particolarmente disinvolta, successivamente, si è assistito ad un progressivo mutamento dei rapporti con le funzioni di business anche a seguito di regole e vigilanze sempre più pregnanti.

Così le funzioni di organizzazione iniziano a configurare le policy aziendali con il supporto di quelle di compliance, individuando l'interesse della clientela come vincolo sin dalla definizione delle stesse. La pianificazione commerciale involge il controllo di conformità per evitare la fissazione di obiettivi non coerenti con i bisogni della clientela servita. La configurazione dei prodotti da offrire non può determinarsi in assenza di parere favorevole della funzione. I sistemi di remunerazione beneficiano del contributo della funzione per evitare spinte a condotte opportunistiche a danno dei clienti.

Nell'intento del legislatore che è progressivamente intervenuto in misura sempre più mirata nella definizione del ruolo della Funzione di Compliance (si pensi da ultimo alle Linee Guida ESMA del 2021 in materia), la correttezza e la trasparenza del comportamento degli intermediari vanno infatti colte nella loro dimensione: (i) strategica, in termini di politiche commerciali e modelli di servizio implementati; (ii) funzionale-organizzativa, con riferimento all' assetto procedurale definito e (iii) operativa, intesa con riguardo alle condotte concretamente poste in essere dai soggetti delle strutture.

Nel quadro appena delineato, la Funzione di Compliance è chiamata dunque ad operare su più livelli, in un costante dialogo con le altre funzioni aziendali, anche di business, con skills e know-how sempre più specifiche, per far fronte alle sfide emergenti, determinate, tra le altre, dall'avanzare a ritmi serrati dell'innovazione tecnologica.

3. Le applicazioni dell'intelligenza artificiale

L'Intelligenza Artificiale risulta una delle principali aree di investimento da parte degli operatori bancari nei prossimi anni, sia a supporto di processi interni, in particolare della Compliance e della prevenzione di frodi, sia per la gestione della relazione con i clienti.

Proprio con riferimento a tale ultimo aspetto, le aree che le Funzioni di Controllo di Conformità sono chiamate a monitorare con sempre crescente attenzione, riguardano in particolare:

Servizio clienti e assistenza: i sistemi basati su chatbot ed assistenti virtuali consentono di gestire in maniera più efficiente le richieste dei clienti, attraverso risposte istantanee e assistenza personalizzata. Tali sistemi interagiscono con la clientela per questioni principalmente inerenti ai saldi dei conti, alla cronologia delle transazioni, riducendo il carico di lavoro "umano".

Servizi di consulenza finanziaria (robo-advice), realizzati, come noto, attraverso diversi modelli organizzativi e di business che spaziano tra (i) l'automatizzazione del servizio in tutte le sue fasi (c.d. robo-advice puro), (ii) la combinazione tra l'elemento umano e quello digitale in una o più fasi della catena del valore (c.d. robo-advice ibrido) e (iii) la fornitura agli addetti dell'intermediario degli strumenti automatizzati a supporto del servizio (c.d. robo-for-advisor), qualificandosi pertanto come B2B (business to business). I diversi approcci coniugano dunque vari livelli di intensità dell'interazione umana nell'attività di consulenza.

Marketing personalizzato: i meccanismi basati sull'intelligenza artificiale sono in grado di elaborare enormi moli di dati dei clienti, derivanti da fonti disparate, per comprenderne le attitudini in modo da definire iniziative di marketing sempre più mirate.

Conformità normativa e reporting: i sistemi di intelligenza artificiale generativa risultano particolarmente utili per supportare gli operatori nella realizzazione di report normativi, principalmente attraverso l'automatizzazione delle fasi di estrazione e organizzazione dei dati e delle informazioni rilevanti.

Il ricorso all'intelligenza artificiale nel settore finanziario presenta diverse sfide e potenziali limiti che devono essere gestiti e affrontati con cautela e attenzione da parte dei controllers, in particolare connessi a:

– privacy: nell'impiego di sistemi di intelligenza artificiale generativa sono necessarie attente cautele per garantire la conformità a normative come il GDPR, per la protezione delle informazioni sensibili dei clienti;
– qualità dei dati: l'utilizzo di modelli di intelligenza artificiale richiede lo sviluppo di articolati processi di monitoraggio e di aggiornamento per il costante utilizzo di dati accurati e affidabili, in grado di produrre risultati attendibili e unbiased; gli algoritmi su cu si fondano tali modelli, se addestrati su dati storici distorti o non aggiornati, possono infatti proporre soluzioni non ottimali;
– trasparenza dei modelli: l'articolazione di tali sistemi risulta spesso poco trasparente (cd. "black box"), e di difficile ricostruibilità ex-post. Si pensi al caso dei robo-advisor che si fondano su algoritmi per costruire, gestire e riequilibrare portafogli di investimento su misura per gli obiettivi dell'investitore. L'opacità nel funzionamento di tali sistemi può dunque rendere difficile valutare la fondatezza delle raccomandazioni e la neutralità dei processi decisionali, in primis da parte dalle Funzioni di controllo, e poi da parte delle Autorità. È pertanto necessario una costante attenzione da parte delle Funzioni di

Compliance al rispetto dei requisiti di trasparenza informativa e di tracciabilità alla base delle raccomandazioni fornite all'utente per evitare il rischio di raccomandazioni non pienamente personalizzate, potenziali conflitti di interesse incorporati nel modello, difficoltà di dimostrare a posteriori il rispetto degli obblighi di *best interest e suitability*. Tale situazione si pone in modo amplificato in caso di outsourcing dei modelli; in questo caso vi è il concreto rischio che l'operatore autorizzato si spogli di ogni competenza in merito svuotando anche di efficacia le attività di controllo, che non possono accedere a tutte le informazioni o comunque non sono in grado di approfondire le modalità di conduzione delle attività esternalizzate;

– robustezza dei modelli: il funzionamento dei sistemi di intelligenza artificiale durante i rispettivi cicli di vita deve avvenire in modo sicuro e protetto e la valutazione/gestione dei potenziali rischi devono essere effettuata nel continuo, in quanto la scarsa affidabilità e accuratezza dei relativi output impatta negativamente sui processi in cui sono impiegati. Si pensi, ancora una volta a titolo esemplificativo, al caso della consulenza automatizzata. La profilazione dell'utente e la valutazione di adeguatezza delle raccomandazioni sono centrali nel quadro normativo dettato dalla MiFID II. Come risulta degli esiti di molteplici studi in materia, gli utilizzatori di robo-advisor dichiarano spesso una fiducia superiore alle reali competenze finanziarie, comportando dunque l'assoluta necessità per gli operatori di garantire percorsi di profilazione robusti e di evitare una fiducia eccessiva nell'automazione, anche nell'ottica di evitare fenomeni di *misselling*.

4. Le piattaforme tecnologiche e l'interazione tra diversi attori

Un altro tema innovativo particolarmente rilevante è quello delle piattaforme tecnologiche utilizzate per l'interazione con la clientela.

Esse sono diventate ormai un driver commerciale importante che può assorbire e assimilare gli operatori tradizionali, finanziari in certi casi, o comunque trasformare il modo di relazionarsi con i clienti.

In termini più generali, tali piattaforme sono considerate da taluni studiosi come il paradigma economico-tecnologico che costituisce il vero propulsore alla base di questo moto di innovazione e (ri)orientamento dei servizi finanziari. Il termine piattaforma, nato in ambito informatico, viene oggi a livello più generale correntemente impiegato per descrivere quelle

infrastrutture digitali che consentono l'interazione fra due o più gruppi/soggetti di diversa natura (consumatori, inserzionisti, fornitori di servizi, produttori, fornitori e financo oggetti fisici). Ancora, esse possono porsi come mero fornitore tecnologico, che si limita a fornire un'infrastruttura digitale agli operatori interessati, ovvero svolgere parti via via più rilevanti delle transazioni finanziarie.

Queste entità stanno portando, nel campo finanziario, ad un crescente scolorimento dei confini tradizionali fra prestatori delle attività riservate e fornitori di servizi informatici.

La rapidità dell'evoluzione tecnologica alla quale stiamo assistendo e il crescente moltiplicarsi delle possibili applicazioni dell'intelligenza artificiale può comportare un effetto di spiazzamento degli operatori, soprattutto di minori dimensioni, incapaci di condurre internamente gli investimenti necessari agli sviluppi informatici sempre più intensi, ma anche carenti del know-how per controllare le attività di fornitori terzi.

Tale situazione sta sempre più frequentemente determinando l'affidamento totale da parte di tali soggetti a provider tecnologici esterni per lo svolgimento di un'ampia serie di servizi, spesso anche di natura core. In questo ribaltamento dei rapporti di forza, può determinarsi una crescente preminenza del fornitore tecnologico rispetto al soggetto vigilato, con la conseguente diffusione di nuovi modelli di business da analizzare e monitorare con sempre maggiore attenzione per evitare la diffusione di "aree grigie" sottratte alla vigilanza.

Secondo quanto emerge dalle evidenze disponibili, tali piattaforme tecnologiche operano con accordi di vario tipo con le istituzioni finanziarie tradizionali; tali collaborazioni riguardano, a titolo esemplificativo, la fornitura di interfacce per la distribuzione di prodotti e servizi, la registrazione e l'elaborazione di dati, l'offerta di soluzioni tecnologiche più innovative, fino ad arrivare in taluni casi alla prestazione diretta di porzioni rilevanti dei servizi.

In taluni casi diviene difficile per il cliente del servizio finanziario distinguere l'entità che presta il servizio riservato rispetto a quelle che mettono a disposizione la tecnologia, comunque desiderose di visibilità e dunque di esporre il proprio marchio verso i clienti per renderlo conoscibile.

Allo stesso modo, piattaforme finanziarie predisposte per lo svolgimento di determinate attività sono utilizzate per promuovere altre tipologie di attività riservate.

Nel contesto descritto appare ancora centrale la figura della compliance, che deve contribuire a disegnare con chiarezza i confini entro cui sono svolte tali attività, controllandone poi il corretto esplicarsi.

5. Il marketing tramite social media/influencer

Da ultimo, ulteriori effetti che l'innovazione digitale sta recando in modo sempre più rapido e dirompente attengono alle modalità di interazione con la clientela nei servizi finanziari.

Oggigiorno, l'accesso alla rete internet avviene in modalità "*everywhere, anytime*", miliardi di persone sono sempre connesse e si è espansa a dismisura la capacità di eseguire transazioni disparate, in tempo reale, attraverso dispositivi di ogni tipo (pc, telefono, orologio, tablet…), con crescente velocità e facilità.

In tale contesto, gli operatori sviluppano modalità e tecniche di sollecitazione commerciale sempre più pervasive, intrusive, talora subdole.

Dunque, anche soggetti particolarmente vulnerabili, ma che tradizionalmente sarebbero meno facilmente "avvicinabili", sono esposti ai rischi di non avvedute scelte finanziarie spinti da tali sollecitazioni.

L'effetto sorpresa, connotato di tutte le offerte che si volgono al di fuori dei locali ove il proponente conduce la sua attività tipica, assume qui rilievo centrale, in quanto il destinatario delle spinte commerciali può essere "aggredito" 24h/24h, in qualsiasi punto del mondo ed in qualsiasi condizione fisica/mentale egli si trovi.

Un ambito in cui tale fenomeno si manifesta con particolare evidenza è quello delle comunicazioni di marketing, con specifico riferimento a quelle oggi veicolate attraverso i social network (Facebook, Instagram, X, Tik Tok). Altro fenomeno che, nello stesso ambito, sta acquisendo crescente rilevanza e che innalza la portata persuasiva del marketing tramite canali innovativi riguarda la diffusione delle comunicazioni pubblicitarie negli stessi social network tramite i cd. "finfluencers", persone note e molto seguite nell'"infosfera" che diffondono contenuti relativi a possibili investimenti.

I suggerimenti di tali soggetti sono accolti con un accentuato affidamento da parte dei destinatari, tipicamente costituiti da ammiratori/fans, anche quando travalicano l'ambito consueto in cui essi si esercitano per diffondersi in modo pervasivo agli aspetti finanziari.

Tutto quanto sopra rende evidente l'assoluta necessità di un'attenzione rafforzata da parte delle strutture di Compliance per assicurare che tali comunicazioni siano chiare, corrette e non fuorvianti in ottica di investor protection. In uno dei passaggi del *Technical Advice on the European Commission mandate on certain aspects relating to retail investor protection* dell'aprile 2022, l'ESMA evidenzia in particolare come "*firms' control functions and senior management must be more deeply engaged in ensuring the regulatory compliance of these*

communications", ponendo dunque particolare enfasi sulla necessità di dedicati focus su tali nuove forme di marketing.

6. Conclusioni

Al termine di questo excursus sul tema, resta qualche spunto di riflessione per le Funzioni di Compliance: bisogna ridisegnare i processi di controllo in conseguenza della riconfigurazione dei business, soprattutto per le realtà più dinamiche; ciò determina la necessità di un conseguente adeguamento delle skills a disposizione della funzione per far fronte all'evoluzione tecnologica. Parimenti è necessario un costante e crescente dialogo, ancora di più rispetto al passato tra la funzione di Compliance e le altre funzioni di business o altre funzioni di controllo aziendali in una prospettiva di parità. Da ultimo, anche per la funzione di compliance sarà importantissimo garantire una corretta gestione ed utilizzo della mole enorme dei dati disponibili in una prospettiva di miglioramento dell'efficienza e dell'efficacia dell'attività.

Il nuovo assetto dell'antiriciclaggio dell'Unione europea: potenzialità, problemi e prospettive

Enzo Serata
Direttore dell'UIF - Unità di Informazione Finanziaria per l'Italia

Nella presente relazione mi occuperò di un tema di particolare attualità nell'ambito della prevenzione e del contrasto del riciclaggio e del finanziamento del terrorismo, vale a dire il nuovo contesto europeo dell'antiriciclaggio, rispetto al quale tutti i soggetti obbligati e tutte le autorità competenti sono oggi chiamati a confrontarsi.

Muoviamo dalla constatazione che, in Europa, nonostante l'emanazione di cinque direttive nel corso di oltre tre decenni, ci troviamo ancora in una situazione caratterizzata da un grado di armonizzazione complessivamente limitato e da significative difformità nell'efficacia della collaborazione attiva; difformità che riguardano aspetti fondamentali quali il contenuto delle segnalazioni – e dunque cosa segnalare – e l'individuazione dei soggetti tenuti agli obblighi antiriciclaggio. Anche le *Financial Intelligence Units* (FIU) operanti a livello europeo presentano caratteristiche fortemente differenziate: alcune sono incardinate all'interno di ministeri o organismi di polizia, mentre altre hanno una matrice prevalentemente amministrativa.

Questa frammentazione, che investe anche l'attività di supervisione in materia di antiriciclaggio, ha prodotto ripercussioni rilevanti sull'efficacia della collaborazione tra le FIU stesse, nonché sulla capacità di individuare tempestivamente anomalie e casi sospetti.

Ne abbiamo avuto una dimostrazione concreta in occasione di diversi scandali e vere e proprie situazioni di crisi bancarie che si sono verificate negli anni passati riconducibili proprio a gravi carenze nei presìdi antiriciclaggio. Il nuovo sistema delle regole europee mira, pertanto, a intervenire su due profili fondamentali: da un lato, l'introduzione di un nuovo "rulebook" armonizzato, fondato questa volta su regolamenti direttamente applicabili e non più su direttive; dall'altro, la creazione di un nuovo sistema sovranazionale di controlli, incentrato sulla nuova Autorità europea, l'AMLA.

In realtà, per quanto concerne le unità di informazioni finanziaria, tale meccanismo non nasce all'improvviso. Già dal 2006, le FIU europee, coordinate dalla Commissione europea, erano state riunite in un gruppo in-

formale con l'obiettivo di agevolare la cooperazione tra le FIU stesse e di svolgere analisi congiunte in casi transfrontalieri. Nel 2015, la quarta direttiva antiriciclaggio riconosce formalmente questa piattaforma delle Financial Intelligence Unit dell'Unione, attribuendole una base giuridica. Nel 2016, la piattaforma ha condotto un esercizio di mappatura degli assetti delle FIU a livello europeo, individuando, già in quella sede, esigenze di armonizzazione e di allineamento delle prassi a standard di maggiore efficacia.

La quinta direttiva, nel 2018, ha inoltre imposto alla Commissione europea di valutare il quadro della cooperazione tra le FIU, le problematiche che caratterizzavano tale sistema e l'opportunità di istituire un meccanismo di coordinamento e supporto delle FIU. La Commissione ha pubblicato un rapporto specifico nel 2019 e, a partire da tale esperienza, ha preso forma l'idea del pacchetto antiriciclaggio europeo.

Il pacchetto è costituito, come noto, da tre regolamenti, segnando l'abbandono dell'approccio che lasciava ampi margini di autonomia agli Stati membri nell'attuazione delle disposizioni. In particolare, un regolamento (UE/2023/1113) disciplina la tracciabilità dei flussi finanziari, con specifico riferimento alle cripto-attività, ed è già applicabile dal 2024; un secondo regolamento (UE/2024/1624) definisce il "*rulebook*" europeo, ossia le norme cui i soggetti obbligati devono attenersi nello svolgimento delle attività di prevenzione e segnalazione delle operazioni sospette; un terzo regolamento (UE/2024/1620) concerne l'istituzione della nuova Autorità europea, l'AMLA, con sede a Francoforte. Il quadro è completato da una direttiva (UE/2024/1640) che lascia agli Stati membri la possibilità di disciplinare alcune aree non direttamente coperte dai regolamenti.

La struttura dell'AMLA presenta elementi di significativa originalità rispetto alle altre agenzie europee. Sotto un'unica architettura istituzionale convivono infatti due funzioni principali: quella della supervisione antiriciclaggio, nella quale l'AMLA assume responsabilità più ampie, e quella del coordinamento delle FIU, ambito nel quale l'Autorità non esercita funzioni operative dirette, ma svolge un ruolo essenziale di indirizzo e coordinamento.

La governance presenta una configurazione peculiare, articolata in due General Board, uno dedicato alla supervisione e uno al meccanismo delle FIU, che presidiano i due "pilastri" dell'Autorità. Accanto a essi opera un *Executive Board*, composto da sei membri, con un ruolo particolarmente rilevante nell'ambito della vigilanza diretta e indiretta, mentre non interviene direttamente sul versante delle FIU. È inoltre previsto un *Executive Director*, responsabile del bilancio, del personale, degli appalti e della gestione amministrativa, nonché un *Administrative Board of Review*, che svolge una funzione di revisione interna delle decisioni adottate dall'AMLA nei

confronti dei soggetti sottoposti alla sua vigilanza. Come noto, nel corso del 2025 la dott.ssa Bruna Szego, della Banca d'Italia, ha assunto il ruolo di presidente dell'AMLA ed è stata completata la selezione degli altri membri dell'*Executive Board*.

La nuova Autorità è dotata di poteri regolamentari significativi. In particolare, sarà chiamata a emanare un numero molto elevato di linee guida e atti di regolamentazione di secondo livello, che riguarderanno sia la supervisione sia il meccanismo delle FIU. Analogamente a quanto avviene nel Meccanismo di Vigilanza Unico, l'Autorità eserciterà poteri di vigilanza diretta su un numero selezionato di intermediari finanziari e disporrà, in casi eccezionali, di poteri sostitutivi nei confronti delle autorità nazionali qualora la loro vigilanza risulti inefficace. È inoltre previsto un potere di supervisione indiretta sul settore finanziario e di *oversight* anche sul settore non finanziario.

A metà del 2025 è stata avviata l'attività dell'AMLA, concentrandosi in particolare sulla supervisione indiretta, sul settore non finanziario e sul coordinamento del meccanismo delle FIU.

Nei prossimi anni sono previsti passaggi di particolare rilievo, soprattutto con riferimento alla supervisione. Nel 2026 dovranno essere definiti i criteri e le metodologie per l'individuazione degli intermediari da sottoporre a vigilanza diretta. Si tratta di un esercizio complesso, poiché la selezione dovrà tener conto della dimensione degli intermediari, della loro operatività transfrontaliera e del profilo di rischio, garantendo al contempo un'adeguata copertura geografica. Sulla base di tali criteri verrà avviata la selezione dei soggetti, con l'avvio effettivo della vigilanza diretta previsto dal 2028.

La prima metà del 2025 è stata caratterizzata da una fase di avvio particolarmente impegnativa, una vera e propria fase di "start-up", volta a costruire la macchina organizzativa dell'Autorità. Sono state avviate le infrastrutture fisiche e amministrative, definita la governance, svolte le prime riunioni del General Board ed è in corso un'intensa attività di selezione del personale. Entro la fine dell'anno l'AMLA dovrebbe raggiungere le 120 unità di personale, destinate a raddoppiare entro la fine del 2026, per arrivare a regime a circa 430 risorse tra il 2028 e il 2029. Parallelamente, sono state avviate le attività preparatorie delle funzioni operative; in particolare, il sistema informatico rappresenta un aspetto di estrema complessità e delicatezza, considerato l'elevatissimo livello di riservatezza delle informazioni trattate.

Sul versante della supervisione, nella seconda metà del 2025 è stata avviata un'attività di ricognizione delle prassi di vigilanza nei diversi Paesi e la formazione dei collegi di supervisione in ambito AML. È stato inoltre avviato un progetto congiunto su alcune aree ritenute a rischio elevato, in

particolare sui prestatori di servizi per le cripto-attività (CASP), accompagnato da una comunicazione dell'Autorità che sottolinea l'importanza di una supervisione efficace su tali soggetti.

Esistono tuttavia ulteriori aree di rischio che meritano particolare attenzione. Una riguarda le società operanti nei sistemi di pagamento, un ambito estremamente variegato e frammentato, nel quale i rischi di riciclaggio risultano elevati per la difficoltà di tracciare in modo efficace i flussi informativi. Un'altra area rilevante è quella dell'utilizzo dell'intelligenza artificiale a fini criminali e, di converso, dell'uso di questi strumenti a supporto della supervisione e delle FIU, ambito nel quale l'AMLA può svolgere un ruolo importante a beneficio delle autorità nazionali.

Per quanto riguarda il versante FIU, sono state avviate diverse attività. Sono state definite le modalità di svolgimento delle c.d. "peer review", ossia le valutazioni degli assetti delle FIU europee condotte dall'AMLA con il coinvolgimento delle FIU nazionali; sono state approvate le procedure di mediazione in caso di conflitti tra FIU; sono state avviate le attività preparatorie per le analisi congiunte, attraverso la definizione degli aspetti metodologici, la ricognizione delle aree di rischio prioritarie e la previsione di un progetto pilota che dovrebbe partire nel prossimo anno. Sono inoltre stati costituiti gruppi di lavoro per la definizione della regolamentazione di secondo livello.

È essenziale precisare che l'AMLA non è una FIU: non riceve né analizza segnalazioni di operazioni sospette, attività che restano integralmente di competenza delle FIU nazionali. Non sono neppure previsti rapporti diretti tra l'AMLA e i soggetti segnalanti, sebbene vi saranno impatti indiretti rilevanti sull'operatività di questi ultimi connessi con i poteri regolamentari della nuova Autorità. Ciò nondimeno il suo ruolo di indirizzo e coordinamento è di cruciale importanza per migliorare l'attività di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo delle FIU dell'Unione.

Uno degli aspetti sui quali si è posta maggiore enfasi nella fase di elaborazione del pacchetto regolamentare europeo riguarda le analisi congiunte. L'esperienza maturata mostra come tali analisi siano difficili da condurre in un contesto caratterizzato da forte eterogeneità tra le FIU. I tempi di realizzazione sono spesso lunghi e l'efficacia complessiva risulta limitata; da qui le elevate aspettative riposte nel ruolo dell'AMLA in questo ambito.

L'Autorità sarà inoltre chiamata a gestire la rete FIU.net, utilizzata per lo scambio di informazioni tra le FIU a livello europeo, e a sviluppare strumenti informatici e metodologici avanzati a beneficio di tutte le FIU.

Tra gli interventi prioritari in materia regolamentare, da completare

nel 2026, rientra l'armonizzazione dei formati delle segnalazioni di operazioni sospette, delle registrazioni di dati interne ai soggetti obbligati, degli scambi informativi tra FIU, nonché delle segnalazioni transfrontaliere. Si tratta di un passaggio cruciale, destinato a incidere profondamente sui sistemi nazionali in quanto può comportare costi di adeguamento significativi sia per le FU sia per i soggetti obbligati, soprattutto per le giurisdizioni meno avanzate. È prevedibile che su questi profili emergano resistenze e tensioni, che richiederanno un'attenta gestione da parte della nuova autorità.

Nel 2027 dovranno inoltre essere emanati indicatori di anomalia a livello europeo, che andranno ad affiancare gli indicatori nazionali, e dovranno essere definite le modalità di trasferimento della piattaforma FIU.net dalla Commissione europea all'AMLA. Altre attività sono previste per il 2028 e il 2029, che avranno un impatto più contenuto rispetto a questa fase iniziale.

Passando a considerazioni di carattere generale, le opportunità offerte dal nuovo assetto sono rilevanti. Nell'ambito del meccanismo di coordinamento delle FIU ci si attende un progresso significativo in termini di armonizzazione, innovazione e rafforzamento degli standard, nonché un miglioramento delle analisi congiunte e della cooperazione transfrontaliera.

Un elemento di particolare rilievo è rappresentato dalla collocazione, sotto un'unica Autorità, della supervisione e del coordinamento delle FIU, che consente di sfruttare importanti sinergie. Dall'attività delle FIU emergono infatti frequentemente criticità riferite non solo a singoli soggetti, ma anche a fenomeni di carattere generale che possono richiedere interventi normativi a livello europeo. In questo senso, l'AMLA potrà dialogare con i legislatori europei con un'efficacia decisamente superiore a quella dei singoli Stati membri. Ci si attende inoltre che la nuova Autorità diventi, nel corso del tempo, un centro di competenze di alto livello, con un ruolo rilevante anche sul piano internazionale.

A fronte di tali opportunità, vi sono tuttavia rischi non trascurabili, legati in particolare ai costi di transizione, soprattutto per le giurisdizioni meno avanzate, chiamate a adeguare i propri sistemi di compliance e di gestione delle informazioni.

La fase di transizione del nuovo assetto europeo sarà lunga e complessa e si svolge in un contesto caratterizzato da una rapida evoluzione tecnologica e da una criminalità economica sempre più sofisticata, con il rischio per le autorità, quanto meno nel breve periodo, di perdere terreno rispetto all'evoluzione dei fenomeni criminali. Sul settore non finanziario, in particolare, l'AMLA sarà chiamata a definire linee guida e regole generali in un comparto tradizionalmente caratterizzato da livelli più bassi di colla-

borazione attiva, perseguendo un non facile bilanciamento tra l'esigenza di rafforzare la compliance e l'applicazione di criteri di proporzionalità e di semplificazione. Un ulteriore profilo di rischio riguarda il cumulo di aspettative e di impegni che gravano sull'AMLA nella fase di avvio, con potenziali riflessi anche sul piano reputazionale.

In conclusione, l'AMLA è chiamata a operare in un contesto internazionale e geopolitico particolarmente complesso. Proprio per questo è essenziale sfruttare questa opportunità storica per rafforzare a livello europeo la prevenzione del riciclaggio e del finanziamento del terrorismo, assicurando una protezione più efficace del sistema finanziario ed economico dell'Unione dalle infiltrazioni criminali.

La sfida principale consisterà nel bilanciare due esigenze contrapposte: evitare un eccessivo accentramento e una standardizzazione troppo rapida, che rischierebbero di generare resistenze, e al tempo stesso evitare l'adozione di standard troppo laschi o tempi di adeguamento troppo lunghi, che pregiudicherebbero il raggiungimento di adeguati livelli di efficacia e di omogeneizzazione dell'attività di prevenzione e contrasto del riciclaggio. È necessario che l'AMLA non rinunci a perseguire obiettivi ambiziosi, puntando all'allineamento alle migliori pratiche e accompagnando le giurisdizioni più in difficoltà attraverso un processo di adeguamento graduale; percorso questo che potrà essere tanto più efficace quanto più l'Autorità saprà valorizzare l'esperienza delle giurisdizioni e delle FIU che hanno investito maggiormente nel rafforzamento dei sistemi di intelligence finanziaria e nel coinvolgimento di un'ampia platea di soggetti obbligati.

Modelli distributivi complessi ed esternalizzazione. La funzione di compliance nelle compagnie assicurative e la tutela effettiva del cliente

Ida Mercanti
Segretario Generale IVASS

1. Introduzione

Ringrazio AICOM per l'invito a partecipare a questo convegno che mi ha fornito l'occasione per svolgere alcune riflessioni sulla funzione di compliance dalla prospettiva, per me nuova, della vigilanza assicurativa.

Molte delle considerazioni che condividerò con voi quest'oggi derivano proprio dall'analisi delle caratteristiche comuni e dei tratti distintivi della funzione di *compliance* nel settore bancario e in quello assicurativo. Infatti, sebbene la compliance sia venuta alla luce nelle normative bancarie, essa ha ben presto varcato la soglia del settore assicurativo, trovando immediatamente posto tra le funzioni fondamentali, cosiddette "*key f*unctions", della governance di una compagnia assicurativa, ossia quelle funzioni senza le quali non sarebbe possibile fare attività assicurativa.

La compliance assicurativa è diventata "adulta" molto prima del trascorrere dei 18/20 anni che oggi celebriamo con riferimento alle normative bancarie. La Direttiva Solvency II risale al 2009 ma è entrata in vigore solo 10 anni fa, nel gennaio 2016.

L'articolo 46 della Direttiva (recepito nel Codice delle Assicurazioni Private, CAP, all'art. 30-quater) le assegna obiettivi chiave: consulenza all'organo con funzioni strategiche sul rispetto delle disposizioni legislative, regolamentari e amministrative; valutazione del possibile impatto di qualsiasi variazione del quadro giuridico sulle operazioni dell'impresa; identificazione e valutazione del rischio di mancata conformità.

Se non bastasse questo pur ampio perimetro d'azione tracciato dalla Direttiva, l'art. 270 degli Atti Delegati Solvency II indica esplicitamente che la funzione di compliance, nel definire il proprio programma di lavoro, deve tenere conto di tutte le attività svolte dalle imprese di assicurazione e di riassicurazione e della loro esposizione al rischio di mancata conformità.

L'amplissimo mandato per la funzione di conformità assicurativa definito dalla normativa europea spiega perché l'IVASS – consapevole della

numerosità e della varietà dei rischi che un assicuratore attivo nei rami vita e danni si trova ad assumere (deliberatamente) e a gestire (responsabilmente) – ha emanato assai tempestivamente il regolamento sul governo aziendale delle imprese assicurative dettagliando e specificando ulteriormente il mandato, i compiti, i metodi, i requisiti e lo standing di tale funzione.

Mi soffermerò in seguito sulla regolamentazione IVASS dedicata alla funzione di conformità; mi preme innanzitutto ricordare due questioni: in campo assicurativo la compliance è stata costretta ad avere una infanzia e un'adolescenza molto più brevi che in altri settori; IVASS ha sempre creduto che fosse necessario non solo definire le responsabilità della funzione, ma supportarla, anche con l'esercizio dei propri poteri regolamentari, nell'acquisire uno standing centrale nell'ambito delle funzioni fondamentali dell'impresa assicurativa, facendone non solo una centrale e indispensabile linea di difesa interna, ma anche un interlocutore qualificato e affidabile della vigilanza.

Possiamo dire che nell'ultimo decennio la *compliance* nel settore finanziario si è effettivamente irrobustita e rafforzata, uscendo da quello status di funzione di controllo interno di secondo piano in cui si trovava all'inizio della propria storia, appunto un ventennio fa. Dobbiamo anche riconoscere che nello stesso lasso di tempo le sono stati attribuiti sempre nuovi compiti, anche in ragione della crescente complessità del business finanziario, delle interrelazioni tra i rischi che il medesimo affronta, dei legami che si vengono a creare tra i diversi attori, dei nuovi paradigmi tecnologici che servono per rimanere sul mercato in modo competitivo. A quest'ultimo riguardo non posso che convenire su quanto è stato poc'anzi autorevolmente ricordato circa l'impatto atteso sulla *compliance* che deriva dal diffondersi rapidissimo dell'intelligenza artificiale nel settore finanziario.

Credo sia assolutamente necessario continuare a sostenere, anche come co-regolatori del settore finanziario, lo sviluppo e il rafforzamento di tale funzione, del suo status, delle competenze di cui può disporre, della sua indipendenza all'interno delle aziende finanziarie.

L'autorità di vigilanza, che dispone di risorse limitate, ha bisogno di un alleato forte, ossia una funzione di conformità robusta, competente, in grado di supportare adeguatamente il board nelle scelte strategiche, di assistere il *management* nella definizione degli assetti organizzativi e delle scelte operative, di "evitare" alle funzioni commerciali inciampi o errori. Soprattutto, la funzione di conformità deve essere (messa) in grado di impostare le relazioni con la clientela non perseguendo obiettivi di formale rispetto delle norme, ma per proteggere l'asset più importante dell'industria assicurativa: la reputazione. Le compagnie preservano la propria reputa-

zione non soltanto perché considerate realtà solvibili e robuste in quanto ben patrimonializzate, ma anche (e soprattutto) perché meritevoli di fiducia; ad esse si affida il delicato ruolo di consulenti nelle scelte finanziarie, e assicurative, a protezione dei nostri beni, del nostro patrimonio, della salute nostra e dei nostri affetti.

La reputazione è un concetto intertemporale: la credibilità e la fiducia si costruiscono nel tempo, con interazioni ripetute: lo sanno bene gli assicuratori che sono definiti investitori istituzionali di lungo periodo.

Per questo la funzione di conformità è chiave nel settore assicurativo: non tanto perché aiuta a investire oculatamente nel lungo periodo, ma perché deve aiutare *management* e azionisti a preservare nel tempo l'asset fondamentale del business assicurativo: il rapporto fiduciario con la clientela. Questa chiede sì rendimenti che consentano di mantenere il proprio stile di vita anche dopo la fine del lavoro attivo, ma soprattutto protezione, lungo tutto l'arco della propria vita, contro gli eventi avversi. Una funzione di compliance forte, autorevole e ascoltata non è dunque solo un prezioso alleato della vigilanza, è il migliore viatico per tutelare la competitività e sostenibilità di lungo periodo dell'impresa.

Ho condiviso finora le mie riflessioni sul ruolo della compliance. Vengono da uno sguardo relativamente "fresco" verso il settore assicurativo. Mi soffermerò ora su alcune considerazioni più tecniche, approfondendo le questioni normativo-regolamentari.

2. Evoluzione del ruolo della funzione di compliance e il rischio di *misconduct*

La funzione di compliance viene identificata, nell'ambito del sistema di controlli interni dell'impresa, come presidio di controllo della conformità, volto ad assicurare la piena osservanza delle normative che disciplinano attività aziendali e comportamenti. In particolare, la compliance è chiamata dalla regolamentazione assicurativa sulla governance a garantire l'osservanza delle norme relative alla trasparenza e correttezza dei comportamenti nei confronti degli assicurati e danneggiati, con particolare riguardo all'informativa precontrattuale e contrattuale e alla corretta esecuzione dei contratti (anche nella fase di gestione dei sinistri).

Il rischio di non compliance è infatti potenzialmente molto pervasivo e richiede l'attivazione di controlli *ex ante* da parte della funzione.

Occorre a ben vedere un approccio proattivo che operi sull'impianto dei processi e degli assetti organizzativi per assicurare che siano coe-

renti con l'obiettivo di sostanziale rispetto delle norme. Va, in questa prospettiva, integrato il ruolo tradizionale di presidio organizzativo per la gestione dei rischi di conformità in quello di consulente del board per il processo di pianificazione strategica aziendale. Essa non è più solo "centro di costo" e strumento di verifica della regolarità formale dell'attività, ma assume rilevanza in termini di supporto alla definizione di strategie aziendali orientate alla correttezza sostanziale della conduzione d'impresa, alla creazione di valore e di salvaguardia del rapporto di fiducia tra impresa e assicurato. Dunque, la valenza di tale funzione, con sempre maggiore convinzione, si innalza a strategica.

È importante che un corretto approccio alla *compliance* parta dal vertice dell'impresa. Una cultura aziendale diffusa in tutta la struttura organizzativa e nei processi aziendali che valorizzi l'integrità della condotta e in cui il vertice aziendale e il top *management* guidino con l'esempio. La compliance diviene quindi componente essenziale della cultura aziendale, pervade tutta la struttura.

3. Ruolo della compliance nella normativa assicurativa

Una specifica responsabilità della compliance è prevista in materia di verifica delle politiche di remunerazione e di politiche e procedure di distribuzione.

Sul primo aspetto, rileva il contributo della funzione alla definizione di politiche di incentivazione e remunerazione che promuovano e favoriscano elevati livelli di integrità e di cultura aziendale collegati al raggiungimento di obiettivi strategici e di creazione di valore per l'impresa, secondo misure di redditività corrette per il rischio.

Inoltre, la disciplina dettata dal Regolamento IVASS in materia di governo societario si concentra su alcuni profili di primaria rilevanza per l'adeguato assetto e costituzione della funzione quale linea di difesa preventiva: commitment degli organi di vertice; autonomia e idoneità all'incarico del titolare della funzione e adeguato posizionamento gerarchico; riporto diretto ai vertici aziendali; assegnazione di autorità, risorse e competenze adeguate quali presupposti di indipendenza della funzione; pianificazione dell'attività di monitoraggio dell'esposizione ai rischi di non conformità e informativa ai vertici aziendali; cultura aziendale di *compliance*.

La disciplina regolamentare consente l'articolazione della funzione in coerenza con la specificità aziendale, integrandosi efficacemente in essa e secondo un criterio di proporzionalità.

D'altro canto, l'adozione di modelli organizzativi "decentrati", con la presenza di distinte unità di controllo specializzato, deve sempre essere coerente con l'attribuzione alla compliance della responsabilità sul presidio del rischio di conformità, assicurando a quest'ultima le leve gestionali necessarie al pieno esercizio del proprio ruolo (ad esempio, in termini di definizione delle metodologie di valutazione del rischio, di individuazione e valutazione delle relative procedure, di verifica dell'adeguatezza delle unità specialistiche) e diretta ad assicurare effettività al ruolo di coordinamento e supervisione della *compliance*, e unitarietà al processo di gestione del rischio.

Inoltre, il regolamento governance pone l'accento sull'importanza della collaborazione e coordinamento tra le diverse funzioni di controllo, affinché il presidio dei rischi sia assicurato mediante un'architettura e un sistema che riconduca a unità le analisi svolte e le funzioni di orientamento alla definizione delle strategie d'impresa.

4. Ruolo della funzione di compliance a fronte di modelli distributivi complessi

I conflitti, la transizione ecologica, la rivoluzione digitale, rappresentano profondi mutamenti di contesto che si riflettono sull'evoluzione dei mercati e dei prodotti. Al contempo mutano gli attori del mercato assicurativo (ai distributori "tradizionali" si affiancano nuovi soggetti non regolamentati e ai modelli distributivi classici si associano piattaforme digitali il cui funzionamento non è di agevole comprensione). Tali cambiamenti determinano una sempre maggiore complessità dei modelli di distribuzione in cui l'accresciuta osmosi tra i diversi operatori del mercato rende ancor più complesso il quadro in cui i sistemi di controllo delle imprese sono chiamati a operare.

L'applicazione formale delle norme non è più sufficiente ad assicurare l'equo trattamento di tutti coloro che sono potenziali fruitori di prodotti e servizi assicurativi. Il ruolo proattivo della funzione diventa ancor più centrale, nella fase di costruzione dei prodotti, mediante interventi di controllo *ex ante* per fini di tutela sostanziale degli interessi dei consumatori.

A questo scopo, le previsioni del Regolamento IVASS in materia di governo e controllo dei prodotti assicurativi (c.d. Regolamento POG) rafforzano il ruolo della compliance nel processo di ideazione dei prodotti, al fine di anticipare le valutazioni sulla corretta costruzione del prodotto, dalla progettazione alla commercializzazione, e ne accrescono il ruolo nella fase *ex post* mediante il monitoraggio su sviluppo e revisione periodica delle

procedure e delle misure di governo dei prodotti assicurativi.

Dunque, anche in una prospettiva di prevenzione del *misconduct risk*, la compliance assume un ruolo centrale lungo tutta la filiera del prodotto, dalla ideazione (cd. *compliance by design*) al corretto collocamento (regole di condotta nella distribuzione, conflitti di interesse, adeguati ed effettivi test di *demands and needs*).

Ciò è tanto più importante a fronte di una sempre maggiore complessità dei modelli di distribuzione, che hanno nel tempo subito già una profonda evoluzione, non solo in ragione della diffusione dell'innovazione tecnologica, ma anche per l'iscrizione nel Registro (RUI) di imprese operanti nei settori energetico, della distribuzione e delle telecomunicazioni, nonché di forme di articolazione collaborativa tra gli intermediari che hanno inciso sulla geografia del settore.

In questo contesto, ad esempio, sono state osservate debolezze dei meccanismi del processo di distribuzione che richiedono un rafforzamento dei presidi organizzativi, con particolare riguardo alle funzioni di controllo, per renderli coerenti con dimensione e complessità di tali modelli distributivi, e per tale via mitigare l'esposizione al rischio di *misselling*.

La lettera al mercato sulla POG del 2024, grazie anche agli approfondimenti condotti dalla supervisione, ribadisce il ruolo strategico della funzione nel bilanciamento tra test quantitativi e qualitativi, nonché nelle valutazioni di coerenza tra *target market* e *performance* effettiva dei prodotti. Oltre che in termini di concreta rispondenza del prodotto rispetto alle reali esigenze del potenziale fruitore, la funzione di conformità assume un ruolo centrale nel contributo che può apportare in termini di effettiva trasparenza e comprensibilità del prodotto, di chiarezza e semplicità del linguaggio utilizzato nei contratti, considerata la rilevanza specifica che le previsioni regolamentari di settore pongono rispetto a tali profili. Il consumatore dovrebbe essere messo nelle condizioni di scegliere, con la maggiore consapevolezza possibile, un prodotto coerente con i propri bisogni e rispondente alle proprie esigenze.

Si pone certamente, alla luce di quanto fin qui detto, un tema di competenze, anche dei Supervisori, per garantire una piena sostanziale compliance alle nuove norme, con un'esigenza di connessa pianificazione, anche in termini di investimento, di interventi di reclutamento, formazione e aggiornamento delle risorse professionali adeguate all'assolvimento dei compiti assegnati. L'IVASS in questo contesto si avvale e promuove ogni potenziale sinergia con le altre Autorità, in un'ottica di piena collaborazione e in una prospettiva di valorizzazione del modello di supervisione in essere.

5. Ruolo della funzione di compliance nel presidio dei rischi tecnologici

Il *framework* DORA ha introdotto ulteriori e rafforzati presidi per il governo dei rischi tecnologici (IT), per l'adeguato presidio dei dati e la gestione consapevole dei servizi IT resi da terze parti, estranee al perimetro dei soggetti vigilati. Vi è infatti nel settore dei servizi IT un elemento di potenziale criticità, anche sistemica, derivante dalla forte concentrazione dei fornitori terzi dei servizi digitali, con una crescita nel continuo del rischio di dipendenza dagli stessi rispetto ai quali è rilevante mantenere l'adeguatezza dei presidi di controllo delle imprese.

In questo contesto, l'Istituto è di recente intervenuto con una specifica lettera al mercato per indicare alle imprese le aspettative di vigilanza in tema di *outsourcing*, anche di servizi ICT e di adeguata *governance* dei connessi rischi. Si è richiamata l'attenzione sulla necessità di preservare saldi presidi di pianificazione e monitoraggio dell'esternalizzazione in particolare delle attività e funzioni essenziali e importanti, in modo da valutarne gli impatti sulla qualità del rapporto con gli assicurati, sui rischi di concentrazione e di dipendenza da soggetti esterni, di affidabilità del processo e di coerenza con il modello di business adottato.

Nella valutazione della conformità del modello di esternalizzazione adottato dal quadro normativo e dalle aspettative di vigilanza, l'Istituto si attende un ruolo proattivo e un contributo significativo della funzione c*ompliance*.

Con riferimento all'intelligenza artificiale (AI), l'ambito assicurativo rappresenta certamente un settore elettivo in relazione al tema dei dati – anche sensibili – in ragione della natura delle coperture offerte su vita, salute, per la protezione dai rischi catastrofali e della relativa interpretazione. Numerosi sono gli ambiti in cui l'AI può trovare applicazione migliorando l'efficienza operativa, ottenendo una personalizzazione sempre più mirata dei servizi, creando nuove opportunità di business. Strutture adeguate di governance sono un asset fondamentale per evitare distorsioni algoritmiche, violazioni di privacy, trattamenti discriminatori o una ridotta mutualità delle coperture, consentendo di esercitare responsabilmente i compiti di controllo sull'AI, il cui utilizzo è importante rimanga improntato a criteri di correttezza ed eticità.

Numerose sono le innovazioni normative intervenute sia sul fronte europeo, sia su quello nazionale che richiedono adeguamenti di compliance, tra le quali l'adozione dell'AI Act e della relativa legislazione nazionale.

Inoltre, l'EIOPA ha recentemente rilasciato una *Opinion* in materia di *governanc*e e *risk management* dell'AI che favorisce la convergenza delle

prassi di vigilanza e fornisce chiarimenti sull'interpretazione delle attuali previsioni sui profili citati contenute nella disciplina di settore (Solvency II e IDD) nel caso di utilizzo di sistemi di AI.

6. Ruolo della funzione di compliance e l'arbitro assicurativo

Un breve cenno alla recente definizione della cornice normativa, prodromica all'ormai prossimo avvio di operatività dell'Arbitro Assicurativo. Anche con riferimento ad esso, è rilevante il ruolo della funzione di compliance, in termini di impostazione dell'azione dell'impresa – e della rete distributiva di cui si avvale – alla corretta gestione della relazione con il cliente per il raggiungimento del migliore interesse dello stesso, come richiede la normativa IDD.

Cruciale sarà al contempo il ruolo della funzione nell'orientare la "retroazione" dell'impresa rispetto al portato delle pronunce dell'arbitro. Ove le stesse, infatti, accertino una condotta deviante rispetto agli standard attesi e alla normativa a tutela del consumatore, la *compliance* sarà chiamata ad intervenire nell'ambito dei processi e procedure aziendali in modo da riorientare l'agire dell'impresa verso la piena conformità con il *framework* di interesse.

Anche le pronunce dell'Arbitro Assicurativo potranno quindi costituire un riferimento per la funzione di conformità, aiutando la stessa e l'impresa di cui è funzione fondamentale a riorientare le proprie prassi a tutela della propria reputazione e, in ultima istanza, del rapporto fiduciario con la clientela.

Avremo sicuramente modo di verificare se l'Arbitro Assicurativo si confermerà, come auspichiamo, un prezioso alleato della funzione di conformità, di cui oggi festeggiamo la maggiore età sia anagrafica sia, e lo dico convintamente, "ideale".

Nuove disposizioni concernenti i fornitori di servizi critici e importanti e il cosiddetto 3rd parties' risk

Francesco Mauro
Head of Unit Supervisory Review, Recovery and Resolution – EBA

È un onore intervenire oggi su un tema che sta assumendo un ruolo sempre più centrale nelle discussioni sugli approcci regolamentari, di vigilanza e delle imprese, nel presidio dei rischi e nella tutela della stabilità finanziaria: la gestione del rischio di terze parti.

In un'era definita dalla trasformazione digitale e dalle interdipendenze globali, una efficace gestione del rischio di terze parti diventa un imperativo strategico. Le imprese attive nei mercati finanziari si affidano infatti sempre più a terze parti per la prestazione di servizi critici o importanti, nella giusta ricerca di maggiore efficienza. Il compito di regolatori, supervisori e sistemi di controllo interno è fare in modo che le potenziali vulnerabilità legate a questa accresciuta dipendenza siano individuate, misurate e gestite.

Le evidenze più recenti sono confermate dal Rapporto di Valutazione del Rischio dell'EBA pubblicato a giugno del 2025 che evidenzia come il rischio operativo sia in aumento: i requisiti patrimoniali per il rischio operativo rappresentano ora il 10,5% dei requisiti patrimoniali totali, spinti da digitalizzazione e dipendenze da terze parti. Parallelamente, il rischio informatico mostra un trend in crescita, un terzo delle banche ha subito almeno un attacco informatico riuscito nella seconda metà del 2024, rispetto al 24% registrato nella prima metà dello stesso anno.

Inoltre, la percezione del rischio di terze parti rimane significativa, mentre le banche segnalano una crescente dipendenza da fornitori ICT e non ICT.

In questo mio intervento cercherò di dare una visione olistica del tema delle terze parti in un panorama regolamentare globale ed europeo attraverso cui non è sempre semplice districarsi e dove diversi concetti affini ma non sempre coincidenti sono emersi o si sono evoluti per cercare di intercettare nel modo più efficace l'emersione e lo sviluppo dei rischi sottostanti.

Nel delineare l'evoluzione dei concetti rilevanti ai fini della gestione del rischio di terze parti a livello globale è possibile individuare tre fasi principali:

– In una prima fase precedente al 2018, l'attenzione si concentra in modo relativamente circoscritto sul rischio di outsourcing e sui presidi contrattuali. In particolare, nel 2005 – Joint Forum (BCBS-IOSCO-IAIS) disegna le fondamenta della gestione del rischio di outsourcing, focalizzandosi sui presidi contrattuali e sulla governance dei servizi critici. Il punto critico è segnato dall'uso estensivo dell'outsourcing da parte delle banche che genera preoccupazione sui temi di *business continuity* e di compliance con la regolamentazione esistente.
– In una seconda fase, dal 2018 al 2021, l'attenzione dei *global standard setter* si sposta verso le dipendenze tecnologiche, in particolare nei confronti dei fornitori di servizi cloud; e al contempo al rischio di concentrazione che già emergeva come connotato di questi specifici servizi e che innesca valutazioni di resilienza che vanno al di là del singolo contratto. In questo contesto, si collocano il rapporto "*FSB Report on Third-Party Dependencies in Cloud Services*" del 2019 e il "*FSB Discussion Paper on Supervisory Issues*" del 2020.
– In una terza fase, dal 2021 in poi, si impone l'esigenza di sviluppare un quadro completo di gestione del rischio di terze parti, fondato su chiari principi generali sulla resilienza operativa. Un punto di svolta è rappresentato dal paper del 2021 "*BCBS Principles on Operational Resilience*", che introduce il concetto di resilienza operativa e che intende segnare un'evoluzione della tradizionale gestione del rischio operativo, spinta anche dalla frequenza di eventi sistemici (es. cyberattacchi, pandemia COVID-19, blocchi di fornitura di servizi essenziali).

L'idea è passare da un approccio puramente preventivo a uno olistico, che garantisca la capacità di resistere, rispondere e riprendersi da interruzioni senza compromettere i servizi critici. Questo implica integrare governance, tecnologia, processi e fornitori in un unico framework di continuità e adattamento.

Il "*FSB Report on Enhancing Third-Party Risk Management and Oversight*" del 2023 si inserisce su questa linea per formalizzare pratiche di governance imprese e autorità per ecosistemi di terze parti. Nel 2025 "*Upcoming BCBS Principles for Sound Management of Third-Party Risk*" dovrebbe codificare TPRM standards e completare il quadro, coprendo il cosiddetto *Nth-party risks*, il tema delle interconnessioni e le dipendenze delle infrastrutture critiche.

Il legislatore europeo ha introdotto il regolamento sulla resilienza operativa digitale (DORA), entrata in vigore nel gennaio 2023, con l'obiet-

tivo di consolidare e aggiornare i requisiti in materia di rischi relativi alle ICT services, istituendo un quadro completo e coerente per la resilienza operativa digitale nel settore finanziario, armonizzando anche i requisiti tra diverse normative settoriali.

DORA, applicabile dal 17 gennaio 2025, è un regolamento destinato ad un'ampia gamma di entità finanziarie come banche (banche/istituti di pagamento/IME), imprese di investimento, assicurazioni/fondi pensione.

All'interno di esso si possono individuare una serie di principi fondamentali, in primo luogo, il rischio ICT di terze parti è qualificato come componente integrale del rischio ICT ed è considerato parte del quadro di gestione del rischio ICT; in secondo luogo, le imprese finanziarie rimangono pienamente responsabili della conformità con DORA e alla legislazione finanziaria applicabile anche quando contrattano servizi. Infine, trova applicazione il principio di proporzionalità, ovvero questi requisiti vanno articolati considerando la natura, la scala, la complessità e l'importanza delle dipendenze tecnologiche e dei rischi derivanti dagli accordi contrattuali sull'uso dei servizi ICT.

DORA fissa requisiti in materia di governance, richiedendo alle imprese di definire una strategia obbligatoria per il rischio ICT di terze parti, un registro dei contratti, e viene considerato obbligo anche l'adozione e il riesame periodico di una politica riguardante gli accordi relativi all'uso dei servizi di terze parti. Vengono fissati i requisiti riguardo alla fase contrattuale e precontrattuale, mentre per ciò che concerne il rischio di concentrazione si tratta di valutare il rischio di dipendenza da pochi fornitori ICT o da fornitori non sostituibili, considerare i subappalti e le implicazioni legate a paesi terzi.

Viene fissato anche un quadro di vigilanza a livello UE per fornitori di servizi ICT vengono designati come critici di terze parti, con designazione da parte delle ESA tramite il Comitato Congiunto (*Joint Committee*) e rispetto a questi fornitori critici le autorità di supervisione europee hanno potere di condurre ispezioni e di formulare raccomandazioni. Il quadro di vigilanza mira anche a monitorare il rischio sistemico di concentrazione ICT nell'UE e soprattutto integra, ma non sostituisce, i compiti di gestione del rischio di terze parti (TPRM) delle entità finanziarie.

In vista dell'applicazione di DORA, l'EBA, insieme alle altre ESAs, ha completato diversi mandati (16 in totale) riguardanti la gestione del rischio ICT, gli incidenti ICT, il testing dei sistemi ICT, i rischi legati a terze parti ICT e la loro supervisione, tutti entro le scadenze e riflettendo i feedback delle consultazioni con gli stakeholder, in particolare per garantire un approccio proporzionato e basato sul rischio.

L'entrata in vigore di DORA ha portato l'UE all'avanguardia nella

implementazione dei nuovi principi sull'*operational resilience* e sulla gestione del *third party risk* sul versante ICT, superando i principi che erano definiti nella GL su outsourcing.

Ma ha anche reso evidente il bisogno di rivedere il trattamento che le stesse linee guida assicuravano per i servizi non ICT. Con questo *background*, l'EBA è intervenuta sulle precedenti linee guida in materia di outsourcing con l'obiettivo di garantire un'applicazione più omogenea e coerente della gestione del rischio derivante da terze parti. L'intervento ha introdotto nuove definizioni – come quella di accordo con terzi parti e di rischio di terze parti – aggiornandole ed allineandole alla luce di DORA; in quest'ottica sono state eliminate le disposizioni ormai integralmente coperte da DORA come le parti relative e al cloud. Le linee guida inoltre sono state ampliate nel loro ambito di applicazione per includere la maggior parte delle entità finanziarie del settore bancario e tengono conto, per quanto possibile, del lavoro di Basilea/FSB.

La bozza di orientamenti EBA sul non ICT TPRM che è stata messa in consultazione lo scorso luglio riprende l'articolazione di DORA, ma anche dei precedenti orientamenti sull'outsourcing, secondo le tappe tipiche di un accordo con terze parti, ciascuna accompagnata da raccomandazioni minime coerenti con un monitoraggio efficace dei rischi e con la piena responsabilità sull'adempimento degli obblighi che resta in capo agli enti finanziari (principio già menzionato, non nuovo ma già cardine nell'ambito dell'esternalizzazione).

In particolare, prima di concludere un accordo contrattuale con terze parti, le imprese finanziare devono individuare e valutare i rischi pertinenti, compreso il rischio di concentrazione, ma anche il rischio geopolitico; devono determinare il carattere importante o essenziale di una funzione con l'ausilio di criteri individuati dalle stesse linee guida. E devono svolgere una due diligence nella selezione e nella valutazione delle potenziali terze parti, includendo il ricorso eventuale a *subcontractors* da parte del *provider* di funzioni critiche o importanti, la capacità di garantire l'efficacia dei propri diritti in materia di audit e ispezioni.

La seconda fase è la stipulazione di un contratto scritto con la terza parte, che prevede la specificazione dei diritti e obblighi di ciascuna delle parti, che include quindi le descrizioni complete del livello di servizio e degli obiettivi prestazionali quantitativi e qualitativi, per consentire senza indebito ritardo adeguate azioni correttive qualora i livelli di servizio concordati non siano raggiunti; i diritti di accesso e di audit in quanto le imprese finanziarie hanno spesso incontrato e incontrano ancora difficoltà nel negoziare le condizioni contrattuali. Ed infine, disposizioni che impongono

alla terza parte di fornire assistenza in caso di incidenti.

Il terzo step è quello del monitoraggio dove le entità finanziarie sono tenute a monitorare su base continua le performance e la conformità delle terze parti attraverso i KPI ma anche attraverso misure di reporting e di controllo interno al fine di identificare insufficienze e a verificare l'efficacia delle misure adottate per risolverle. La propria capacità di monitorare le funzioni critiche ed importanti in caso di catene di *subcontrators* potenzialmente lunghe o complesse è cruciale.

L'ultimo step del *life cycle* riguarda le strategie di uscita. Il piano di uscita deve essere documentato e realistico, con un calendario di attuazione compatibile con le condizioni contrattuali.

La bozza di orientamenti include poi prescrizioni specifiche sulla governance delle imprese che ovviamente interessano da vicino le funzioni di controllo, inclusa quella di compliance: in particolare, fondamentale quella riguardante l'obbligo del Consiglio di amministrazione di adottare e di rivedere periodicamente una politica in materia di gestione dei rischi di parti terze. La politica dovrebbe definire o indicare una metodologia per determinare quali servizi supportano una funzione essenziale o importante.

Al fine di garantire un monitoraggio efficace, le imprese finanziarie devono avere risorse, competenze e conoscenze sufficienti del personale incaricato e devono assicurare una corretta allocazione delle responsabilità interne, nell'ambito del sistema di controllo interno.

Con i nuovi Orientamenti sulla revisione prudenziale, ora in fase di pubblica consultazione, la resilienza operativa sarà integrata anche nello SREP - *Supervisory of Review and Evaluation Process*", facendo leva sulla valutazione che il supervisore opera sulla governance interna e sul rischio operativo (principalmente continuità operativa, gestione dei cambiamenti, servizi di terze parti e ICT).

La gestione del rischio di terze parti (TPRM) sarà operata secondo un approccio integrato, articolato sui seguenti pilastri:

– Analisi del Modello di Business: valutazione preliminare delle dipendenze strategiche dai fornitori.
– Governance Interna: verifica della coerenza delle politiche di TPRM e dell'efficacia dei presidi di controllo interno.
– Rischio Operativo e ICT: monitoraggio costante tramite l'analisi degli incidenti relativi a terze parti, simulazioni di scenari di interruzione (BCM) e test di resilienza mirati.
– Resilienza Operativa: mappatura delle interdipendenze esterne per garantire la continuità delle funzioni critiche e importanti anche in caso di disservizi dei partner.

In conclusione, *Operational resilience* e TPRM pongono sfide tanto difficili quanto cruciali per imprese, autorità di vigilanza e regolatori su cui ci siamo dilungati nella relazione. L'EBA sta cercando e continuerà a cercare di inquadrare queste sfide in un ambito di regole allineate agli standard internazionali ma anche coerenti, che promuovano la resilienza del sistema ma anche requisiti e un quadro di vigilanza proporzionati e integrati.

I commenti che abbiamo ricevuto nelle varie consultazioni ci confermano che questa è la strada giusta, e ci danno suggerimenti preziosi che ci aiuteranno a finalizzare i documenti. Ovviamente, definire regole adeguate è complicato, farle rispettare, dalle funzioni di controllo interno (compliance in primis) e dalle autorità di vigilanza, sarà una sfida ancora più importante che l'EBA senz'altro supporterà nell'ambito della propria attività di monitoraggio e promozione della convergenza nell'UE.

TAVOLA ROTONDA

L'evoluzione della funzione compliance: tecnologia e innovazione come motore di sviluppo sostenibile

Alberto Pezzi
Professore Ordinario di Economia e gestione delle imprese - Università degli Studi Roma Tre

Piero Boccassino
Senior Consultant del CEO e già Chief Compliance Officer – Gruppo Intesa Sanpaolo

Raffaele Panìco
Risk & Compliance Officer – Gruppo Poste Italiane

Marco Rossetti
Group Chief Compliance Officer – Banca Mediolanum

Antonio Graziano
Responsabile Antiriciclaggio – Gruppo Poste Italiane

Massimo Rella
Direttore Crediti – Banca Mediolanum

PROF. PEZZI – Buongiorno a tutti, la tavola rotonda odierna si propone di approfondire i temi trattati dalle Autorità durante la mattinata, adottando un approccio prevalentemente operativo. L'obiettivo centrale è tracciare l'evoluzione della funzione compliance, con un focus specifico sulla tecnologia intesa come motore di sviluppo sano, sostenibile e duraturo della funzione stessa.

Nel corso del dibattito, verrà analizzato come l'innovazione possa supportare i processi di controllo, senza tuttavia trascurare le criticità e le preoccupazioni che l'adozione di nuovi strumenti tecnologici può sollevare nella gestione quotidiana delle numerose attività di controllo e di compliance.

Partecipano alla tavola rotonda: il dottor Piero Boccassino, Senior Consultant del CEO e Chief Compliance Officer del Gruppo Intesa Sanpaolo, il dottor Antonio Graziano, responsabile Antiriciclaggio del Gruppo

Poste Italiane, il dottor Raffaele Panìco, responsabile Risk e Compliance del Gruppo Poste Italiane, il dottor Massimo Rella, direttore crediti di Banca Mediolanum ed il dottor Marco Rossetti, Group Chief Compliance Officer di Banca Mediolanum.

Iniziamo il confronto partendo dal Dottor Piero Boccassino. Alla luce del contesto attuale, in che modo e in quali ambiti l'innovazione può esprimere il suo massimo potenziale per la funzione compliance, sia nell'immediato che, soprattutto, in un'ottica di medio-lungo periodo.

Dott. Boccassino – Buongiorno a tutti, innanzitutto ringrazio l'avvocato Cola e il professor Pezzi per l'invito che è particolarmente gradito ed è l'occasione per parlare di temi che sono estremamente significativi.

Questa mattina abbiamo ascoltato la voce delle Autorità che sicuramente è la base di partenza per i nostri ragionamenti. La prima cosa che mi sento di dire è che il tema della tecnologia, la relazione tra tecnologia e compliance si pone su due ambiti: la funzione di conformità assieme al risk management hanno un ruolo essenziale nella gestione del rischio collegato alla tecnologia, però nel contempo la funzione di conformità è fruitrice della tecnologia e deve sicuramente utilizzarla per evolversi.

Andando con ordine, qualche riflessione riguarda la gestione del rischio, perché chiaramente il rischio collegato alla tecnologia ha una valenza normativa, nel senso che la norma è pervasiva e da lì nasce la funzione di conformità e il suo ruolo.

Quali sono gli ambiti normativi in cui sussiste questo collegamento?

Sicuramente il primo che viene in mente è quello collegato all'intelligenza artificiale che è sicuramente un aspetto di grande rilevanza con risvolti normativi.

Il secondo è quello legato ai profili di sicurezza e di protezione dei dati; mentre il terzo che è stato tra l'altro ampiamente sviluppato questa mattina dal rappresentante dell'EBA, il dottor Mauro, è quello legato alla gestione dei fornitori terzi di servizi IT.

Infine, il quarto e ultimo, in qualche modo è collegato alla tecnologia, è l'ambito relativo a prodotti e servizi che vengono grazie alla tecnologia e qui c'è tutto il mondo degli asset digitali.

Andando con ordine sull'intelligenza artificiale cercherò di essere breve per ragioni di tempo, sicuramente tutte le nostre realtà stanno investendo nell'intelligenza artificiale che crea grandi opportunità ma chiaramente anche dei rischi che devono essere presidiati.

Come Intesa San Paolo, noi abbiamo ad oggi più di duecento "use

case" che fanno ricorso all'intelligenza artificiale, ma anche le altre istituzioni finanziarie si trovano nella stessa situazione.

Chiaramente, la funzione di conformità deve garantire che l'adozione dell'IA avvenga in modo conforme alla norma. A livello europeo, per l'AI Act (*Artificial Intelligence Act*) ci sarà una rimodulazione dei tempi di entrata in vigore di alcuni aspetti; restano però centrali i temi della gestione dei rischi, come la non discriminazione, la trasparenza (o spiegabilità) e la sorveglianza umana. Il ruolo della compliance è cruciale, dato che esistono ambiti ad alto rischio come il credito, i servizi assicurativi e la gestione del personale.

Se con l'IA tradizionale il compito è più semplice, con l'IA generativa o agentica la complessità aumenta. Sicurezza, resilienza e protezione dei dati sono temi complessi coperti, per il settore finanziario, dal regolamento DORA e, a livello *cross industry*, dalla direttiva NIS2. In particolare, DORA si focalizza molto sulla gestione delle terze parti, di cui si è parlato questa mattina ed è un tema estremamente rilevante. Infine, il rispetto del GDPR richiede un ruolo attivo della funzione di conformità, all'interno della quale viene spesso inserito il *Data Protection Officer* (DPO).

Sull'utilizzo dei servizi di terzi, integrando l'intervento del dottor Francesco Mauro, la funzione di conformità deve operare su due livelli: la governance complessiva e il controllo sui singoli fornitori.

A livello di governance, è essenziale definire una strategia complessiva per i rischi informatici, garantire l'aggiornamento del registro e assicurare un coinvolgimento costante degli organi societari.

Sui singoli fornitori, invece, l'attenzione si sposta sull'*assessment* iniziale e sulla definizione degli obblighi contrattuali. È fondamentale presidiare l'intero ciclo di vita del rapporto, dall'avvio fino alla exit strategy: un elemento critico che, sebbene difficile da attuare concretamente, resta indispensabile.

Un tema centrale è il rischio di concentrazione e del rischio sistemico. I fornitori strategici sono numericamente limitati e prevalentemente di estrazione statunitense. Per far fronte a ciò, il regolamento DORA ha introdotto la possibilità per le tre autorità europee (EBA, ESMA ed EIOPA) di intervenire direttamente su tali fornitori. Recentemente è stato pubblicato il primo elenco di società considerate critiche (tra cui Google e Amazon), su cui verrà esercitata questa nuova azione di vigilanza. Poi, in concreto bisogna andare a vedere come verrà esercitata tale attività di vigilanza.

Infine, sul fronte della gestione del rischio, non si può ignorare il tema dei crypto-asset, regolati dai framework MiFID o MiCA a seconda dell'ambito di applicazione. La compliance deve abbracciare l'evoluzione tecnologica, specialmente nei settori dove la gestione dei dati è vitale. Mi

riferisco in particolare all'Anti-Financial Crime e al Market Abuse, ambiti nei quali – con Intesa Sanpaolo in prima fila – si stanno concentrando investimenti significativi per rendere i controlli sempre più evoluti.

Prof. Pezzi – Ringrazio il Dottor Boccassino per le riflessioni di grande interesse. Riprendendo un tema emerso durante la mattinata, appare evidente come il contesto attuale richieda la gestione di realtà estremamente complesse.

In termini di complessità, il Gruppo Poste Italiane rappresenta un caso esemplare: un'organizzazione caratterizzata da una vasta presenza territoriale e da un'offerta integrata di servizi finanziari e non finanziari. Tale eterogeneità accresce inevitabilmente il peso della sfida regolamentare.

Rivolgo quindi la parola al Dottor Raffaele Panìco: quali sono le soluzioni organizzative adottate dalla funzione Compliance per gestire efficacemente questa complessità industriale e normativa?

Dott. Panìco – Buongiorno a tutti, ringrazio il professor Pezzi e l'avv. Cola, inizio citando un concetto che ripetiamo spesso in Poste Italiane: al nostro Gruppo si applica quasi l'intero ordinamento giuridico, sia nazionale che europeo. Come anticipato dal Professor Pezzi, ci siamo allontanati tanto da quella che era l'attività principale di Poste, quella logistica fondamentalmente, e abbracciato settori un tempo distanti dal nostro core business, che oggi è diventato prevalentemente finanziario.

Siamo dunque soggetti a normative cogenti, tipiche dei settori vigilati come quello bancario e assicurativo, che ci impongono un costante adeguamento. Tuttavia, come è stato sottolineato più volte stamattina, la compliance non va intesa semplicemente come un "mettersi in regola", ma come un vero volano per il business.

Se vogliamo che agisca come motore della crescita, la funzione di conformità deve essere organizzata in modo da rispondere non solo agli obblighi di legge, ma alle reali esigenze strategiche dell'azienda.

La survey Aicom-Protiviti di fine 2024 sulla funzione compliance in aree non finanziarie, citata dal dott. Clemente, evidenzia come la maggioranza delle aziende adotti un modello accentrato. Anche il nostro è un modello accentrato, declinandosi però in una forma "mista": il presidio centrale è la funzione di Risk Compliance di Gruppo.

Non si tratta di semplice compliance, ma di una struttura integrata che comprende:

– Risk Management e Compliance di Gruppo;
– Presidi relativi al D.Lgs. 231/2001;
– Funzioni Antifrode.

L'obiettivo di questa struttura è armonizzare l'attività dei nostri "compliance specialist", equilibrando le linee di indirizzo centrale con l'operatività specifica dei vari settori, senza che l'autonomia di una parte schiacci l'altra.

Un aspetto cruciale riguarda l'analisi delle variazioni normative. In Poste adottiamo una modalità multi-compliance: le norme non vengono mai analizzate in modo settoriale o isolato, ma congiuntamente da tutte le strutture interessate. Questo approccio omogeneo serve a evitare ridondanze e a garantire uniformità d'azione. Non mi soffermo sulle metodologie tecniche – non siamo qui per una lezione accademica e chi mi ha preceduto lo ha spiegato egregiamente – ma sottolineo l'importanza di raggiungere un efficiente risultato operativo.

Qualche anno fa abbiamo fatto una scelta strategica: distinguere tra norme cogenti (a cui non ci si può sottrarre) e certificazioni volontarie. Abbiamo deciso di metterci alla prova con la ISO 37301, che certifica il sistema di gestione della conformità. Per noi non è una semplice certificazione o un obbligo di legge, ma un modo per sfidare noi stessi, accettando il rigore di un certificatore esterno per validare la qualità del nostro modello.

Dico spesso ai miei colleghi: abbiamo voluto intraprendere questo percorso e ora ne gestiamo le conseguenze, ma si tratta di ricadute costruttive e migliorative. Sottoporsi a standard così rigorosi obbliga a innalzare il livello, preparando l'azienda a sfide diverse e permettendo di potenziare il sistema di controllo nella sua interezza.

Un esempio pratico è la *legal inventory* richiesta dalla ISO 37301: un'attività che forse non avremmo mai avviato spontaneamente, ma che oggi conta ben 3.000 righe di analisi. Questo strumento è prezioso sia a livello globale che per i singoli *compliance specialist*, perché fornisce loro una guida per orientarsi correttamente di fronte ai nuovi scenari. È un approccio che, chiaramente, non può prescindere dal supporto della tecnologia.

Prof. Pezzi – Il tema della regolamentazione si intreccia inevitabilmente con quello della complessità normativa che, in molti contesti, viene ancora percepita come un potenziale freno all'innovazione. In questo scenario, rivolgo una riflessione al Dottor Marco Rossetti: quanto è prioritario oggi per un istituto bancario adottare un approccio strutturato nell'utilizzo delle nuove tecnologie? E, parallelamente, qual è l'impatto concreto di questa evoluzione tecnologica sull'operatività della funzione compliance?

Dott. Rossetti – Buongiorno, in primis credo sia doveroso ringraziare AICOM, non solamente per l'invito di oggi, ma soprattutto per il supporto garantito alle funzioni di compliance negli ultimi 20 anni. Mi occupo di

compliance dal 2008 e AICOM è sempre stata al fianco delle funzioni compliance lungo un percorso che è stato particolarmente sfidante.

La complessità normativa è stata una costante nel percorso di sviluppo della funzione compliance. Se pensiamo semplicemente all'ultimo anno, le banche sono state impegnate nell'implementazione di normative importanti e sfidanti quali ad esempio l'*Accessibility Act*, la BCBS239, DORA, ecc.

Si tratta sicuramente di sfide molto importanti, ma se volgiamo il nostro sguardo verso il futuro, senza voler scendere nel tecnico, ci rendiamo conto che l'evoluzione normativa non si è certo fermata. Basti pensare che nei prossimi 3 anni dovremo analizzare ed implementare la RIS, la SIU, la MCD2, la CCD2, la PSD3, l'IA Act, il Listing Act, la FIDA e numerose altre normative fondamentali. Penso che si possa dire che la gestione della complessità è ormai parte del DNA delle funzioni di Conformità!

Questa mattina è stato detto che la funzione compliance è nata per essere una risposta alla complessità. Sicuramente è un auspicio corretto, che ben delinea una possibile linea evolutiva per il ruolo della funzione nel futuro. Tuttavia, credo che, se riconsideriamo l'operato della funzione negli ultimi 20 anni, non sempre sia stato possibile raggiungere in modo soddisfacente tale obiettivo.

Sotto l'egida della funzione compliance, le banche hanno definito corpus documentali più strutturati e puntuali, implementato sistemi di controllo e percorsi formativi che hanno coinvolto tutto il personale aziendale, definito processi di *onboarding* e sensibilizzazione rivolti alle nuove risorse. Tutto ciò ha sicuramente avuto esiti estremamente positivi in termini di *risk culture* e sensibilità interna, ma talvolta ha avuto anche l'effetto collaterale di aumentare ulteriormente il livello di complessità dei processi interni.

La diffusione di nuove tecnologie, in primis l'intelligenza artificiale, a mio parere può permetterci di superare il *trade-off* tra gli obiettivi di riduzione della complessità e di rafforzamento dei presidi interni in materia di conformità normativa.

Tuttavia, se è vero che l'intelligenza artificiale ci permetterà di fare dei passi avanti molto importanti, è tuttavia importante considerare che questo strumento comporterà anche nuove sfide e nuovi rischi. È quindi a mio parere fondamentale che le banche affrontino tale tema nell'ambito di un framework articolato e olistico.

Il primo passo, a mio parere, è lavorare sulle persone. Banca Mediolanum da anni ha messo un focus importante sul concetto di *risk culture*, anche riprendendo gli spunti proposti da BCE nell'ambito della comunicazione del 2024. L'obiettivo è stato in primis lavorare sulla sensibilità delle

nostre persone, perché i dipendenti e i collaboratori di una banca devono rispettare centinaia di regolamenti e procedure. Un approccio nozionistico non può più bastare, è fondamentale che essi sviluppino una spiccata sensibilità ai rischi di carattere normativo. L'attenzione al rischio deve diventare un aspetto della loro quotidianità. A riguardo l'aspetto davvero rilevante è che le nostre persone siano in grado, nel mezzo della gestione delle attività quotidiane, di cogliere il possibile rischio che stanno gestendo e riuscire a farsi la domanda giusta. Saranno poi le strutture preposte all'interno della banca, quali il responsabile diretto, la funzione compliance o le altre funzioni di controllo, a dare supporto alla persona nella gestione del tema potenzialmente rischioso.

Ma tutto passa dalla sensibilità di chi è "in prima linea". Se si riesce a sviluppare questa sensibilità a livello operativo, da questa si può partire per costruire un framework di gestione dell'AI che permetta alle banche di sfruttare al meglio le potenzialità di questa nuova tecnologia, senza incorrere in rischi non governabili.

Permettetemi un inciso, spesso sento dire che l'intelligenza artificiale corre veloce, ed è sicuramente vero. Però credo sia fondamentale che le banche affrontino questa evoluzione tecnologica rispettando i tempi tipici dei processi di trasformazione del mondo bancario, ponendo l'attenzione anche sulle persone che lavorano al loro interno.

Sottolineo infine un ultimo aspetto a mio parere fondamentale, ovvero la qualità dei dati su cui andremo ad implementare l'AI. Sicuramente le banche dispongono di un patrimonio di dati enorme e di grandissimo valore. Tuttavia, le funzioni di compliance, e più in generale le banche, dovranno fare investimenti importanti per poter organizzare al meglio tale patrimonio. In questo percorso sicuramente un riferimento importante è costituito dalle linee guida emanate da BCE in materia di RDARR.

Se le banche saranno in grado di gestire al meglio i propri dati, e mantenere l'alta attenzione da sempre posta sul personale interno, allora l'intelligenza artificiale potrà costituire un supporto importante in termini di riduzione della complessità ed efficacia dei processi interni.

Andando ora ad aspetti maggiormente concreti, la funzione compliance di Banca Mediolanum, che oggi rappresento, attualmente utilizza tre differenti sistemi di intelligenza artificiale nell'ambito dei propri processi di supporto e controllo di conformità. Abbiamo integrato tali sistemi nei nostri processi al fine di supportare al meglio le persone della funzione.

Il primo elemento di AI è stato implementato a supporto delle attività di *legal inventory*, un processo particolarmente sfidante per tutte le funzioni compliance. Successivamente abbiamo investito in relazione all'attività

di pareristica e, più recentemente, abbiamo iniziato ad utilizzare l'AI per lo sviluppo di corsi di formazione più interattivi e personalizzati.

A mio parere questo non è un punto di arrivo, ma il primo passo per avere funzioni di conformità maggiormente efficaci, che non vengano viste come generatori di complessità, ma bensì come una risposta ad essa.

Prof. Pezzi – Ringrazio il Dottor Rossetti per le sue riflessioni. Entriamo ora nel merito di due aree operative fondamentali: l'Antiriciclaggio e la Direzione Crediti. Rivolgo la parola al Dottor Antonio Graziano: quali sono, dal suo punto di vista, le principali innovazioni tecnologiche necessarie per assolvere in modo efficace e moderno alle previsioni normative in materia di antiriciclaggio? Allo stesso modo, vorrei successivamente coinvolgere il Dottor Massimo Rella per capire come l'innovazione stia impattando l'area Crediti, un'area dove il presidio dei rischi e la conformità sono altrettanto centrali.

Dott. Graziano – Prima di entrare il professor Pezzi mi ha suggerito di dare il punto di vista degli operatori dopo aver sentito le istituzioni e quindi tutta l'evoluzione del mondo normativo che ci concerne, a partire dal mondo dell'antiriciclaggio.

Il settore dell'antiriciclaggio (AML) ha vissuto un'evoluzione enorme: partendo dalla Convenzione di Vienna dell'88 e dalle prime norme del 1991, siamo arrivati al D.lgs. 231/2007, che rappresenta la vera pietra miliare. Oggi questa evoluzione corre ancora più veloce, spinta dalle nuove tecnologie e da un confronto costante con le Autorità di vigilanza e giudiziarie, che sempre più spesso accolgono le nostre osservazioni per migliorare il sistema di prevenzione.

Poste Italiane ha scelto un approccio distintivo: la funzione antiriciclaggio è autonoma e separata dalla compliance. Questa scelta riflette la vastità del Gruppo, che comprende player primari in diversi settori:

– BancoPosta (settore finanziario);
– Poste Vita (assicurativo);
– PostePay e la neonata LIS Pay (pagamenti elettronici).

Proprio alcuni di voi durante il break, mi hanno chiesto ma perché Poste è molto coinvolta nel mondo dell'antiriciclaggio? La nostra capillarità sul territorio e la mole di patrimonio amministrato – circa 590 miliardi di euro, di cui 320 nel solo risparmio postale – ci rendono un bersaglio naturale per chi tenta di riciclare denaro. La nostra missione è impedire che i servizi di Poste vengano strumentalizzati per finalità illecite.

La funzione antiriciclaggio cerca di evitare questo rischio, di evitare

che i riciclatori ci utilizzino con queste finalità. Abbiamo creato questa funzione antiriciclaggio di gruppo, per tutto il Gruppo Poste Italiane, proprio per dare un indirizzo comune a tutti i soggetti obbligati. Noi definiamo le politiche antiriciclaggio, definiamo quali sono i processi e le procedure omogenee per tutti i soggetti obbligati del gruppo e siamo il primo interlocutore del consiglio di amministrazione. Un fattore critico di successo è il pieno coinvolgimento del top management: quando il *commitment* verso la legalità arriva dall'alto, il nostro lavoro diventa più incisivo. Oggi, nessuna nuova linea di business, prodotto o canale può essere lanciato senza il via libera" preventivo delle funzioni di controllo.

Noi siamo inseriti, insieme al collega della compliance, in tutte le valutazioni di nuovi prodotti, canali e servizi quindi non passa nulla senza il nostro via libera. Spesso per aiutare il business blocchiamo quelle linee nuove che possono essere pericolose per il gruppo e siamo assolutamente ascoltati all'interno dell'azienda.

Nell'affrontare il rischio, la tecnologia è un'arma a doppio taglio. Da un lato, le nostre controparti la usano con estrema rapidità; con i miei collaboratori spesso li chiamo i nostri docenti, nel senso che noi impariamo da loro, perché spesso vediamo delle attività e l'utilizzo di operatività illegali che non conoscevamo e che ci permettono di migliorare i nostri sistemi di prevenzione. Dall'altro lato, la tecnologia è la nostra difesa principale; non si può pensare di fare prevenzione antiriciclaggio senza il supporto della tecnologia soprattutto con i grandi numeri che lavoriamo quotidianamente.

Tuttavia, in Poste il fattore umano resta centrale: il 60% degli alert sono generati da sistemi informatici; ma il 40% degli alert viene segnalato dalla rete degli uffici postali. Il direttore d'ufficio che "conosce il cliente" resta la base del Know Your Customer (KYC).

Attualmente non utilizziamo ancora un'IA pura, ma operiamo su una piattaforma di Big Data basata su regole deterministiche. Questo ci permette di analizzare l'andamentale del cliente nel tempo e verificare la congruità delle operazioni rispetto al suo profilo finanziario.

Sull'intelligenza artificiale generativa stiamo conducendo valutazioni prudenti. Sebbene possa essere utile nell'automazione della raccolta dati e nell'adeguata verifica, presenta ancora criticità nell'individuazione delle operazioni sospette. Inoltre, il rapporto costi-benefici è centrale: l'innovazione deve essere sostenibile e non deve prescindere dal valore del lavoro umano. Ad oggi, in Poste, è ancora l'uomo ad avere l'ultima parola.

DOTT. RELLA – Buongiorno a tutti, innanzitutto ringrazio per l'invito e facevo una riflessione sulla circostanza che tra tutti i pannellisti e i rappre-

sentati delle autorità di vigilanza sono l'unico responsabile di una struttura di business che genera rischio essendo *Chief landing officer*: quindi se si mette male mi avvarrò della facoltà di non rispondere.

È estremamente interessante analizzare il tema dell'innovazione tecnologica applicata ai processi bancari sotto la lente della compliance, ovvero dal punto di vista della conformità e del controllo dei rischi.

Recentemente è uscito uno studio di Mckinsey che riporta che il 52% dei manager del settore bancario, e in generale finanziario, ritiene l'intelligenza artificiale e l'applicazione dell'intelligenza artificiale nei processi della banca e dei soggetti finanziari una priorità. Lo stesso studio di Mckinsey però ci dà un altro dato estremamente interessante: su cento progetti avviati di intelligenza artificiale, solo cinque trovano poi reale applicazione nei processi. Per due ragioni, uno attiene alla normativa e quindi al rispetto delle norme, perché spesso si parte con un'idea che potrebbe sembrare estremamente brillante, anche in termini di potenziali risultati, poi ci si scontra col fatto che c'è una normativa, giustamente, sottolineo giustamente, da rispettare; l'altra ragione è legata al fatto che spesso chi viene coinvolto nell'ambito dei soggetti finanziari delle banche, nei progetti di implementazione dell'intelligenza artificiale, in particolare quella generativa, cerca l'effetto wow, cioè cerca l'effetto su una micro attività o comunque su un'attività molto limitata senza badare invece al risultato che deve esserci sul processo *end to end*.

Quello che noi stiamo facendo, lavorando in simbiosi con le funzioni di controllo, compliance e risk management e in particolare privacy è quello di dare concretezza alla nostra iniziativa, non cercando l'effetto wow, anche perché come ci ha detto poco fa dal dottor Boccassino, tutte le grandi realtà, tutte le grandi banche hanno cantieri aperti sull'intelligenza artificiale, quindi non ci si inventa nulla come capacità di messa a terra; l'invenzione, la parte più innovativa, viene dalla tecnologia in sé.

Quindi ci interessa la concretezza, per avere concretezza sono tre i temi da mettere in sicurezza: bisogna avere obiettivi chiari e l'obiettivo chiaro per noi vuol dire l'efficacia e l'efficienza dei processi in una visione *end-to-end*, non ci interessa l'effetto speciale.

Il secondo obiettivo è ottenere un ritorno per gli *stakeholder* e in primis, tra questi *stakeholder*, i clienti, perché se non diamo benefici ai clienti l'intelligenza artificiale non serve veramente a nulla, ma non soltanto agli *stakeholder* intesi come i clienti ma anche intesi come i colleghi, i dipendenti, i collaboratori e in questo mi trovo molto d'accordo con quanto detto poco fa dal collega di Poste.

Terzo obiettivo per avere successo e concretezza in un progetto di implementazione di intelligenza artificiale bisogna essere consapevolmente

in grado di assumersi dei rischi, che non vuol dire non assumere dei rischi perché per definizione, se fai impresa assumi dei rischi. Però se assumi rischi consapevolmente vuol dire che sei in grado di saperli identificare e quindi presidiare.

Vedendo a noi, sono tre le funzionalità principali dell'intelligenza artificiale generativa che possono dare un beneficio: 1) la capacità di sintesi e concisione, quindi di riassunto, 2) la capacità di generare autonomamente contenuti e 3) la capacità di ingaggiare i clienti. Queste tre funzionalità ci hanno spinto ad individuare nel settore del credito, quelli che sono i tre ambiti sui quali intelligenza artificiale generativa può essere sviluppata, quindi messa a terra, che sono:

– Early Warning (monitoraggio anticipato), per analizzare preventivamente il comportamento dei clienti e degli imprenditori che hanno finanziamenti in essere.
– Analisi documentale e credit memo, per automatizzare l'esame della documentazione e la generazione delle relazioni istruttorie.
– Customer engagement, per gestire l'interazione con i clienti attraverso chatbot evoluti e altre soluzioni smart.

L'intelligenza artificiale che parla con i clienti, che interagisce per i clienti, ci sono già dei case study utilizzati, applicati o quanto meno studiati anche da banche italiane, mi giro di fianco al collega Boccassino perché so che Intesa ci sta lavorando.

L'oggetto dell'intervento è il processo dei mutui, che presenta caratteristiche ideali per l'integrazione della intelligenza artificiale generativa:

– Volume di dati e documenti: l'istruttoria di un mutuo è estremamente complessa. Incrociando tipologie di prodotto, le diverse tipologie di immobili, profili dei richiedenti e variabili immobiliari, arriviamo ad analizzare oltre 100 documenti per singola pratica.
– Standardizzazione: trattandosi di processi standardizzati, le attività sono ripetitive e si prestano all'automazione.
– Intensità di lavoro: è un processo molto *time-consuming* e *labor-intensive*, che richiede tempi lunghi e il coinvolgimento di molte persone.

L'intervento si concentra sulla fase iniziale dell'istruttoria, dove l'intelligenza artificiale gestisce l'intero ciclo documentale. I documenti vengono acquisiti da un sistema, ma potrebbero essere ricevuti anche via e-mail, che li classifica per tipologia. L'IA controlla la correttezza e la coerenza dei documenti, estraendo i dati necessari. Le informazioni vengono trasferite in una partizione dedicata, dove il sistema esegue verifiche di coerenza interna tra i diversi dati estratti. Poi, il sistema popola automaticamente il gestionale "mutui" con i dati validati. Infine, l'IA produce una

bozza della relazione istruttoria, il cosiddetto Credit Memo.

I controlli dove sono? L'essere umano dove? In ogni fase, ci sono controlli e c'è l'intervento dell'essere umano. Non si passa da una fase all'altra, se non c'è la validazione da parte dell'essere umano. Non si passa da una fase all'altra, se non c'è un controllo sulla verifica, sulla bontà dei dati.

Il processo dei crediti nella banca è uno dei più regolamentati, da sempre. Le banche sono nate per fare credito, per fare intermediazione tra chi ha bisogno di denaro e chi invece vuole prestarlo. Noi siamo vigilati dalla BCE, ma per le banche vigilate dalla Banca d'Italia, la normativa fondamentalmente è la stessa. Le linee guida dell'EBA ci dicono esattamente come fare credito. L'intelligenza artificiale quello deve fare. Deve fare credito come lo farebbe un essere umano.

Perché quindi impieghiamo un anno e mezzo per mettere a terra il progetto? Un progetto che dal punto di vista tecnologico potrebbe essere messo a terra in sei mesi, ma richiede un anno e mezzo? Dobbiamo insegnare all'intelligenza artificiale che le 70 pagine di linee guida dell'EBA sulle "*Loan Origination and Monitoring*", devono essere seguite puntualmente dalla macchina, esattamente come lo farebbe una persona. Quindi, dobbiamo insegnare alla macchina a rispettare la normativa.

Il potenziale sicuramente è enorme in termini di contenimento dei tempi e capacità dell'intelligenza artificiale generativa di essere "multitasking".

Prof. Pezzi – Vi ringrazio per questi spunti preziosi. Da questo primo giro di interventi emerge con chiarezza come la tecnologia sia il fattore abilitante per trasformare le attività di compliance più onerose, puntando a un deciso efficientamento dei processi.

La sfida futura, a mio avviso, risiede nella capacità di integrare i requisiti normativi, destinati a farsi sempre più stringenti nei prossimi anni, direttamente nella fase di progettazione dei processi aziendali. L'obiettivo deve essere quello di superare la logica dei "silos normativi" a favore di una visione sistemica e integrata. Parlo da accademico, consapevole che la messa a terra di questi concetti rappresenti una sfida operativa di non poco conto.

Guardando dunque al futuro, vorrei tornare dal Dottor Panìco: quali sono le soluzioni organizzative e strategiche per integrare efficacemente la funzione Compliance con le diverse aree di business, considerando la vastità e l'eterogeneità dei settori in cui opera una realtà come Poste Italiane?

Dott. Panìco – Riferendosi alla compliance "*by design*" posso dire che Poste è un'azienda in cui il "top management" è illuminato. Sono arrivato

in Poste Italiane 21 anni fa e venivo da una realtà completamente diversa, una realtà militare, dove dai degli ordini e qualcun altro li esegue.

Quando arrivi in una realtà come Poste e cominci a parlare di *security by design*, qualcuno ti guarda con uno sguardo attonito e si chiede perché tu devi intervenire in un processo di costruzione del business.

Le riflessioni condivise convergono verso una medesima direzione; tuttavia, appare di particolare interesse analizzare come, all'interno di processi orientati alla generazione di ricavi, dinamica che caratterizza Poste al pari di ogni altra realtà aziendale, si possa verificare una duplice condizione operativa. In passato, la funzione era percepita come un inibitore del business; attualmente, nella nostra organizzazione, siamo invece considerati abilitatori dei processi. Come osservato in precedenza, la creazione di un prodotto che integri sin dalla genesi le analisi antiriciclaggio, antifrode e la valutazione dei rischi ai sensi del D.Lgs. 231/01, permette di validare il progetto con la massima competenza tecnica disponibile.

Sebbene sia noto che il rischio zero non sia perseguibile, l'obiettivo risiede nella definizione di un rischio gestibile. È necessario che i proponenti del business manifestino con trasparenza le criticità potenziali, con particolare riferimento alle frodi. Il raggiungimento di tale equilibrio in un'organizzazione complessa rappresenta un obiettivo sfidante. Il superamento della logica del mero costo a favore di una piena integrazione della sicurezza nei processi di business segna il conseguimento di un traguardo fondamentale.

L'esperienza pregressa dimostra che l'immissione sul mercato di prodotti senza il preventivo coinvolgimento dei Competence Center, come li chiamiamo noi, ha prodotto esiti negativi, anche sotto il profilo economico: l'onere di correggere carenze strutturali ex post è sensibilmente superiore all'investimento necessario per una corretta progettazione iniziale.

Il passaggio qualitativo consiste nel riconoscere che la sicurezza — intesa come conformità e tutela a 360 gradi — costituisce un vantaggio competitivo per l'azienda, per la clientela e per tutti gli stakeholder. Tale evoluzione deve essere sostenuta da un uso consapevole della tecnologia. La nostra capacità d'investimento, coerente con le dimensioni del Gruppo, rimane costantemente parametrata e misurata in funzione dei ricavi attesi, garantendo così la sostenibilità economica dell'innovazione e della protezione degli asset aziendali.

L'adozione sistematica della tecnologia e dell'Intelligenza Artificiale (IA) all'interno della nostra organizzazione è stata preceduta da un atto fondamentale: la redazione di un Manifesto Etico. Tale documento definisce i criteri e i perimetri d'impiego delle soluzioni di IA per tutta l'azienda,

stabilendo una cornice valoriale imprescindibile.

A supporto di questa visione, è stato istituito un Comitato per l'Intelligenza Artificiale, presieduto dal Direttore Generale. Questo organo collegiale assolve a una duplice funzione:

– Monitoraggio Normativo: Presidio costante delle evoluzioni legislative, con particolare riferimento ai regolamenti dell'Unione Europea.
– Approvazione Progettuale: Valutazione e autorizzazione dei singoli progetti tecnologici, garantendo la coerenza con le strategie aziendali.

Le potenzialità offerte dall'IA sono consolidate: nell'ambito dell'antifrode, ad esempio, gli algoritmi consentono di individuare pattern complessi con una tempestività preclusa all'analisi umana. Tuttavia, l'implementazione tecnologica non prescinde dall'analisi dei rischi critici, quali:

– Bias algoritmici: Il rischio di errori sistematici o distorsioni nei risultati.
– Over-reliance: L'eccessivo affidamento sugli output tecnologici a discapito dello spirito critico.
– La Centralità del Capitale Umano e il Valore Sociale.

In un'azienda che conta 120.000 dipendenti e riveste un profondo valore sociale, l'introduzione dell'IA viene gestita con estrema responsabilità, anche nel dialogo con le rappresentanze sindacali. L'obiettivo strategico non è la riduzione dell'organico, bensì l'efficientamento del tempo lavorativo, permettendo alle persone di concentrarsi su attività a maggior valore aggiunto. Sebbene lo scenario tecnologico sia destinato a evolvere radicalmente nei prossimi anni, l'impegno attuale della società resta saldo: garantire legalità, trasparenza e integrità operativa. In questa visione, la compliance non agisce come freno, ma come volano strategico, integrando l'innovazione tecnologica con la centralità insostituibile delle persone.

Prof. Pezzi – Proseguendo l'analisi del contesto di Poste Italiane, vorrei ora interpellare il Dottor Antonio Graziano. Siamo di fronte a novità normative di portata storica che impatteranno profondamente il comparto: mi riferisco in particolare all'AML Package e alla costituzione dell'AMLA (*Anti-Money Laundering Authority*).

Quali sono le prospettive per il prossimo futuro in termini di evoluzione operativa? Abbiamo già sottolineato come la tecnologia sia fondamentale per l'efficientamento; spesso il dibattito si concentra sulla quantità e sulla qualità delle Segnalazioni di Operazioni Sospette (SOS), ambito in cui l'Intelligenza Artificiale può offrire un contributo determinante.

Al di là del mero efficientamento dei processi esistenti, quali sono i nuovi sviluppi che possiamo attenderci per potenziare concretamente la lotta al crimine finanziario e affinare i presidi antiriciclaggio?

DOTT. GRAZIANO – L'evoluzione del quadro antiriciclaggio di cui abbiamo parlato nel corso dell'intera mattinata è già in corso e procede rapidamente, sia a livello normativo sia purtroppo per quanto riguarda le tecniche utilizzate dai criminali. In questo contesto, una figura chiave sarà l'esponente antiriciclaggio nel Board, prevista dalle nuove norme: una presenza competente all'interno del Consiglio faciliterà la comunicazione con il responsabile Antiriciclaggio, aumenterà la consapevolezza del rischio e rafforzerà processi e procedure. In Poste sarà nominato ad Aprile 2026 in occasione dell'insediamento del nuovo Consiglio di amministrazione, anche se in effetti già da tempo l'AD ed il Direttore generale svolgono questa funzione ai massimi livelli. Tra l'altro la maggior parte dei grandi intermediari italiani hanno già scelto l'amministratore delegato come esponente antiriciclaggio.

Un secondo elemento fondamentale sarà la maggiore integrazione normativa, soprattutto rispetto a privacy e inclusione finanziaria, che oggi creano attriti con le esigenze dell'antiriciclaggio. Oggi all'antiriciclaggio non si richiede soltanto di segnalare operazioni sospette, ma anche di bloccarle, l'evoluzione normativa deve consentire agli operatori un'adeguata copertura giuridica, specialmente nei rapporti con l'autorità giudiziaria.

La tecnologia dovrà permettere di agire ex-ante, in modo proattivo, intervenendo prima che un'operazione rischiosa venga eseguita. L'intelligenza artificiale a mio avviso in futuro potrà aiutare a raggiungere meglio tale obiettivo.

PROF. PEZZI – Riprendo volentieri uno spunto emerso durante la nostra breve interlocuzione in occasione del coffee break - momenti di confronto informale che ritengo fondamentali e assolutamente irrinunciabili in queste occasioni.

Rivolgo la prossima riflessione al Dottor Piero Boccassino, partendo proprio dalle novità introdotte dall'AML Package. Se non erro, l'Articolo 75 introduce il tema cruciale delle partnership: si apre la strada a una forma strutturata di scambio di informazioni tra soggetti privati, nonché tra il settore pubblico e quello privato, coinvolgendo direttamente le Autorità.

Questo paradigma collaborativo rappresenta potenzialmente un punto di svolta per lo sviluppo futuro dei temi che stiamo trattando. Qual è la sua visione su questo nuovo scenario e come crede che influenzerà l'operatività dei grandi gruppi bancari?

Dott. Boccassino – Un tema estremamente rilevante, ma se i tempi lo consentissero, vorrei fare una chiosa sull'utilizzo della tecnologia da parte della conformità. Ritengo che l'impiego della tecnologia, con particolare riferimento all'intelligenza artificiale, rappresenti un requisito imprescindibile per la funzione di conformità. L'evoluzione del settore muove necessariamente in tale direzione, in una prospettiva che considero assolutamente compatibile con la salvaguardia dei livelli occupazionali.

In merito alla mia esperienza presso il Gruppo Intesa Sanpaolo, l'Area Chief Compliance Officer coordina circa 1.500 risorse a livello globale, operando in molteplici geografie con i relativi presidi locali. Se si estende l'analisi alle figure operanti nel sistema di contrasto all'*anti-financial crime* – funzioni esterne alla mia area ma essenziali al raggiungimento degli obiettivi – il numero complessivo supera le 2.000 unità.

Qualora non avessimo implementato una serie di iniziative basate sull'intelligenza artificiale, sarebbe stato necessario un incremento dell'organico nell'ordine di diverse centinaia di unità, in aggiunta a una dimensione già considerevole. Tale esigenza sarebbe scaturita da:

– Evoluzioni normative e indicazioni delle Autorità di Vigilanza.
– Incremento dei settori a rischio e obblighi di monitoraggio rafforzato dei clienti a seguito di Segnalazioni di Operazioni Sospette (SOS).

Abbiamo risposto a tali sfide massimizzando l'uso della tecnologia attraverso un modello ibrido. Attraverso soluzioni custom (Interne) abbiamo adottato l'intelligenza artificiale, anche di tipo generativo, nei processi relativi ai profili autorizzativi di *Know Your Customer* (KYC). In questo ambito, l'IA elabora una proposta decisionale che rimane, in ultima istanza, di competenza umana. Inoltre, tre anni fa abbiamo istituito l'*Anti-Financial Crime Digital Hub*, finalizzato a sviluppare soluzioni di *detection* che hanno fornito risultati eccellenti, in particolare nella gestione del contante.

Attraverso soluzioni di mercato abbiamo acquisito strumenti avanzati per la gestione delle sanzioni finanziarie, per l'analisi dei media (*Adverse Media/Press*) e per la sorveglianza delle comunicazioni, ambito cruciale della compliance regolamentare. Tali tecnologie trovano applicazione anche nel tiering ai fini KYC.

L'adozione di queste soluzioni tecnologiche ha permesso di evitare ulteriori ampliamenti dell'organico, garantendo al contempo l'adeguatezza della struttura rispetto alle crescenti complessità del panorama normativo.

L'articolo 75 del nuovo pacchetto legislativo europeo in materia di antiriciclaggio (AML Package) rappresenta un'opportunità di rilievo, alli-

neando la normativa comunitaria alle migliori pratiche internazionali. Tali forme di cooperazione tra settore pubblico e privato sono già state sperimentate con successo in diverse giurisdizioni, quali Stati Uniti, Messico, Canada e Singapore.

Il rafforzamento della visione d'insieme sui fenomeni criminali, attraverso la condivisione delle conoscenze, costituisce il futuro del contrasto al crimine finanziario. Poiché le attività illecite non si limitano a singoli istituti, è essenziale superare la frammentazione informativa.

Sebbene l'attuazione richieda estrema cautela per garantire il rispetto della privacy e prevenire l'esclusione finanziaria, il percorso tracciato dall'articolo 75 – pur con i limiti attuali che ne circoscrivono l'applicazione ai soli clienti ad alto rischio – permette uno scambio informativo operativo di grande interesse.

L'impegno di Intesa Sanpaolo in questo ambito si articola su due livelli:

– Partnership Strategica. L'Istituto ha promosso, unitamente a Banca d'Italia, UIF, Guardia di Finanza e DIA, una collaborazione strategica nel Nord-Ovest focalizzata sulla condivisione di metodologie. Tale iniziativa, sotto l'impulso di Banca d'Italia e UIF, si sta ora estendendo su scala nazionale con il coinvolgimento dell'ABI.
– Partnership Operativa. L'auspicio è che il quadro delineato dall'articolo 75 possa evolvere ed arricchirsi, favorendo una messa a fattor comune delle informazioni sempre più efficace.

L'obiettivo di tale evoluzione non è esclusivamente l'efficacia nel contrasto al crimine, ma anche l'efficienza dei processi. È fondamentale evitare ridondanze procedurali, a beneficio sia dei soggetti privati che delle autorità pubbliche (come l'UIF), garantendo un sistema di vigilanza snello e incisivo.

Prof. Pezzi – Vorrei ora coinvolgere il Dottor Marco Rossetti su un tema emerso con forza durante la mattinata: la gestione delle terze parti e, sempre più spesso, delle quarte parti (i sub-fornitori). In un ecosistema così interconnesso, la catena di esternalizzazione può estendersi indefinitamente, ponendo sfide inedite.

Come può la funzione Compliance esercitare un controllo efficace su questa filiera? Il problema si complica ulteriormente se consideriamo l'Intelligenza Artificiale: il mercato attuale è estremamente polarizzato e i principali player tecnologici operano spesso al di fuori dei confini europei, che rimangono però il nostro perno regolamentare imprescindibile.

Pur trattandosi di una questione complessa, credo sia fondamentale

offrire alla platea spunti operativi: come si concilia l'adozione di tecnologie globali con il rigore delle normative europee (come l'AI Act e DORA) nella selezione e nel monitoraggio dei fornitori?

Dott. Rossetti – Sicuramente la gestione delle terze e delle quarte parti che collaborano con il sistema bancario è un tema particolarmente attuale e rilevante. Le banche, nel corso dell'ultimo anno, hanno lavorato con impegno e determinazione per raggiungere la piena conformità a quanto richiesto da DORA, in relazione a questo tema.

Vi sono tuttavia alcuni elementi di complessità, credo comuni all'intero sistema bancario, che rendono particolarmente complesso il raggiungimento di un livello di piena rispondenza ai dettami normativi, spesso determinando, almeno nel breve periodo, un rischio di non conformità.

Il primo elemento è la necessità di confrontarci con alcuni fornitori (penso, ad esempio, a servizi di cloud, *infoproviding* e, più recentemente, intelligenza artificiale) che sono player globali, spesso di origine americana. Con tali soggetti è spesso complesso raggiungere accordi contrattuali pienamente rispondenti ai dettami di DORA ed ottenere un accesso adeguato alla loro documentazione interna, ad esempio per quanto attiene alle loro policy di *business continuity* e ai test effettuati, nonché diritti di auditabilità realmente illimitati.

Il secondo elemento importante è disporre di adeguate competenze interne a tutti i livelli, da quelle più specialistiche, ad esempio in cybersecurity e *operational resilience*, fino ad arrivare a quelle strategiche a livello consigliare e di top management, in relazione ad ambiti così tecnici e in fortissima evoluzione.

In relazione a questi ambiti, in questa fase, è fondamentale stimolare all'interno delle Banche un confronto aperto e trasparente, anche a livello di CdA e comitati interni, in modo da poter essere certi che qualsiasi scelta sia effettuata previa un'accurata valutazione degli eventuali rischi residui, in alcuni casi non pienamente mitigabili nell'immediato.

A riguardo vi è un elemento a supporto. Recentemente EBA ha emanato un elenco di un primo gruppo di fornitori strategici su cui le Autorità europee andranno ad attivare un'attività diretta di vigilanza. Questa attività risulterà sicuramente importante per l'intero sistema bancario.

Prof. Pezzi – Per concludere questo primo giro di tavolo, vorrei interpellare il Dottor Massimo Rella, spostando il focus sull'area business. Abbiamo ampiamente discusso di come l'Intelligenza Artificiale e le nuove tecnologie siano, e saranno sempre più, fattori critici di successo per le istituzioni finanziarie.

Da studioso di economia e gestione delle imprese, mi pongo tuttavia una domanda di natura strategica: gli ingenti investimenti tecnologici in atto potrebbero alterare le attuali dinamiche concorrenziali? Come accennato durante la mattinata, stiamo assistendo all'ingresso di nuovi player estremamente aggressivi, che utilizzano leve di marketing e modelli operativi distanti dal mondo bancario tradizionale, rendendo la competizione particolarmente complessa.

Ci troviamo di fronte a una minaccia per chi fatica ad adeguarsi, oppure l'investimento nell'IA diventerà una *commodity* necessaria? In questo secondo scenario, partendo tutti dallo stesso livello tecnologico, l'efficacia degli strumenti adottati diventerà il vero discriminante per risolvere le problematiche operative, tanto nella Compliance quanto nell'area Crediti.

Dott. Rella – È un tema che è estremamente interessante perché tocca anche una affermazione fatta poco fa proprio dal collega Rossetti: il cosiddetto rischio di "compliance". Non tutti lo presidiamo nello stesso modo, questa mattina si è fatto riferimento ad un intermediario senza fare il nome ma penso che l'abbiamo capito tutti chi fosse, che ha fatto della gestione del rischio di "compliance" la chiave del proprio successo; oggi sono arrivati ad avere 65/70 milioni di clienti nel mondo gestendo il rischio di compliance con un appetito che non è esattamente quello di Mediolanum, Intesa, Poste; è un appetito differente che accetta il rischio di non conformità pagando la sanzione, prevedendo degli accantonamenti per il rischio. Quindi il terreno di gioco non è esattamente uguale per tutti, il terreno di gioco non è assolutamente uguale per tutti.

Il terreno è estremamente competitivo oggi e lo sarà sempre di più; poco fa il dottor Boccassino ha già anticipato la nuova frontiera che non è nemmeno più quella dell'intelligenza generativa ma è della intelligenza artificiale agentica che ha delle potenzialità incredibili e che, riprendendo anche i ragionamenti fatti dai colleghi di Poste, può veramente incidere in modo significativo anche sui livelli di occupazione.

Non ci possiamo assolutamente sottrarre da questa incertezza perché c'è sotto fondamentalmente un rischio di business enorme e quando parlo di rischio di business intendo dire rischio di sopravvivenza. Chi oggi non esplora questo terreno rischia il futuro, rischia la sopravvivenza nel futuro.

Oltre alle sfide tecniche, il dibattito attuale si concentra significativamente sulle implicazioni etiche dell'innovazione. In questo contesto, gli investimenti risultano cruciali e devono essere indirizzati in modo sinergico verso tutte le linee di difesa dell'istituto: dalla prima linea (Business e Direzione Crediti) fino alla seconda e terza linea di controllo. È indispensabile

che ogni funzione riceva il medesimo supporto tecnologico per operare al passo con un mercato estremamente dinamico e competitivo.

Nella nostra esperienza, poi, il confronto costante con i principali attori globali dell'innovazione ci pone dinanzi a una frontiera tra il noto e l'ignoto. Le trasformazioni attese non nei prossimi venti, ma nei prossimi cinque anni, saranno radicali, pertanto, è fondamentale presidiare anticipatamente tali cambiamenti.

L'allocazione di capitali nell'innovazione non è solo una scelta strategica, ma un atto di tutela verso tutti gli stakeholder: dagli azionisti alle Autorità di vigilanza, ai clienti, dipendenti e collaboratori.

In conclusione, è necessario che le Autorità di vigilanza operino per garantire un terreno di gioco equo, assicurando che le medesime regole e condizioni competitive siano applicate uniformemente a tutti gli attori del mercato, a fronte dei massicci investimenti richiesti.

Prof. Pezzi – Siamo giunti al termine della tavola rotonda. Desidero ringraziare sentitamente i nostri relatori per aver condiviso non solo la loro visione strategica, ma anche spunti operativi di estremo valore.

È emerso chiaramente che la tecnologia non è più un'opzione, ma il terreno su cui deve correre una compliance moderna. Le prossime sfide, di noi tutti, saranno trasformare queste riflessioni in processi concreti, muovendosi tra le complessità normative dell'AML Package e le potenzialità della tecnologia in particolare dell'intelligenza artificiale.

Ringrazio tutta la platea per l'attenzione e la partecipazione. Con l'auspicio che la giornata di oggi possa essere di supporto nel vostro lavoro quotidiano, dichiaro conclusa questa sessione.

Conclusioni

Alberto Pezzi
Professore Ordinario di Economia e gestione delle imprese - Università degli Studi Roma Tre

Silvia Vicentini
Vice Presidente AICOM – Associazione Italiana Compliance

Il percorso di riflessione sviluppato in tutti gli interventi consente di affermare che la funzione compliance ha ormai definitivamente superato la fase in cui veniva percepita come presidio meramente difensivo, chiamato a intervenire a valle dei processi decisionali o, peggio, a rispondere a delle criticità sopraggiunte.

Dall'esperienza condivisa dagli interventi istituzionali e professionali è emerso, inoltre, che la compliance non viene più vista come un mero "centro di costo" ma si collochi, oggi, all'interno delle dinamiche di governo dell'impresa, come funzione capace di concorrere alla qualità delle decisioni strategiche, alla sostenibilità dei modelli di business e alla tutela della clientela.

A venti anni dal documento del Comitato di Basilea sulla compliance nelle banche, la funzione appare non solo consolidata nei suoi presupposti organizzativi – indipendenza, autorevolezza, adeguatezza delle risorse, accesso alle informazioni, raccordo con gli organi aziendali – ma anche profondamente evoluta nella sua capacità di incidere sui processi di pianificazione, di sviluppo dei prodotti, di gestione dei canali distributivi e di presidio dei nuovi rischi non solo nel settore finanziario. La compliance diventa, quindi, una funzione abilitante non perché riduca l'intensità dei controlli, ma perché rende più solide, consapevoli e sostenibili le scelte di impresa nel medio-lungo periodo.

La transizione dalla compliance formale (controllo della lista delle regole) alla compliance sostanziale e strategica comporta che la conformità non sia più un freno allo sviluppo ma un ingranaggio interno ai processi industriali e operativi. Se grazie alla *compliance by design* un prodotto nasce già conforme, l'impresa ne guadagna in termini di performance (velocità, sicurezza, rischi, ecc.) e reputazione (valore del brand, fiducia del cliente, engagement).

Il nuovo volto della compliance passa per molti degli argomenti trattati dai relatori. In primo luogo, la crescita del ruolo strategico della compliance è strettamente legata alla maggiore articolazione e complessità

del panorama esterno. Il progressivo modificarsi del quadro regolamentare nazionale e internazionale, la rapidità dei mutamenti tecnologici, l'interdipendenza tra soggetti vigilati e fornitori di servizi, la transizione digitale dei servizi, lo sviluppo di nuove forme distributive e l'aumento dei pericoli legati alla reputazione e all'operatività impongono alle strutture aziendali un'evoluzione qualitativa senza precedenti.

La funzione compliance è oggi chiamata a presidiare fenomeni che richiedono competenze interdisciplinari: cyber risk, DORA, AI Act, MiCAR, strategie di comunicazione sui social media, nuove strutture antiriciclaggio, ecc. Ne consegue che ogni iniziativa aziendale rilevante – che si tratti di un nuovo prodotto, di un nuovo canale distributivo, di un processo automatizzato, di un'alleanza con dei fornitori – richiede un coinvolgimento preventivo della funzione di conformità a supporto delle decisioni al fine di evitare che la velocizzazione dei processi decisionali si traduca in vulnerabilità giuridiche, operative o reputazionali che finiscano per distruggere valore piuttosto che crearlo.

In secondo luogo, una traiettoria segnata e in veloce evoluzione riguarda l'interazione tra conformità e tecnologia. La tecnologia è, al tempo stesso, oggetto e strumento del presidio di conformità. È oggetto di presidio perché l'innovazione digitale genera nuovi rischi normativi, organizzativi ed etici: si pensi all'utilizzo dell'intelligenza artificiale nei processi di consulenza, selezione e profilazione della clientela, nelle procedure di monitoraggio dell'antiriciclaggio, gestione della concessione del credito e in genere dei flussi comunicativi. Al contempo, però, la tecnologia funge da strumento di compliance, dato che soltanto attraverso investimenti mirati nel governo dei dati, nei sistemi di automazione, nelle analisi statistiche avanzate e nelle soluzioni di intelligenza artificiale sarà possibile gestire efficacemente l'incremento della pressione normativa e operativa.

Il nuovo petrolio sono i dati e anche la compliance nel futuro prossimo sarà sempre più *data driven*, associando alla capacità di utilizzare i dati per i controlli, l'individuazione di anomalie ed errori, la capacità di prevedere i rischi, calibrare le attività di verifica secondo criteri di priorità (*risk-based*), valutare l'efficacia delle misure adottate, migliorare la qualità della collaborazione con le Autorità di vigilanza. Tuttavia, l'adozione di soluzioni tecnologiche prevalentemente legate all'evoluzione delle varie intelligenze artificiali non coinciderà con la sostituzione del giudizio professionale, ma con il suo potenziamento; molte sono le riflessioni in atto a livello istituzionale e delle singole imprese che mettono correttamente in guardia contro i pericoli legati all'opacità dei processi decisionali delle macchine (black box), ai pregiudizi algoritmici (bias), alla difficoltà di spiegazione dei risul-

tati, alla dipendenza dalle terze parti, al possibile declino della qualità dei dati e alla inevitabile diluizione delle responsabilità.

Un terzo argomento di riflessione strettamente legato ai due precedenti è individuabile nel ruolo centrale delle competenze professionali. La multidisciplinarietà all'interno della funzione sarà necessaria per poter governare competenze di natura giuridica, organizzativa, aziendalistica, tecnologica e comportamentale. Figure professionali con competenze specialistiche dovranno operare con figure professionali polivalenti al fine di mantenere, anche grazie ad una necessaria formazione continua, la funzione all'altezza delle nuove sfide future.

Quarto spunto di riflessione è quello relativo al governo integrato dei rischi. Appare sempre più difficile conciliare una gestione dei rischi per sylos con una sempre più marcata correlazione tra rischio di non conformità, rischio di riciclaggio, rischio operativo, rischio tecnologico, rischio reputazionale, ecc. La compliance mantenendo la necessaria distinzione di ruoli rispetto a risk management, internal audit, antiriciclaggio, cybersecurity e rischio operativo, deve potersi collocare all'interno di un sistema di coordinamento forte, capace di offrire agli organi aziendali una visione chiara e complessiva del profilo di rischio.

In questo scenario, la gestione del rischio derivante dalle terze parti assume un valore crescente. La normativa DORA e le recenti linee guida europee chiariscono inequivocabilmente che delegare un'attività non significa trasferire la relativa responsabilità legale. La trasformazione dei modelli operativi e il ricorso massiccio a fornitori esterni per attività cruciali pongono la compliance di fronte a un nuovo paradigma: vigilare non solo sul perimetro interno, ma su intere catene di dipendenza tecnologica e operativa che si sviluppano all'esterno. Al contrario, quanto più il soggetto vigilato dipende da terzi – e talvolta da quarte parti difficilmente controllabili – tanto più deve rafforzare capacità di selezione, negoziazione contrattuale, monitoraggio, auditabilità, exit strategy e gestione del rischio di concentrazione. In futuro, ciò dovrebbe comportare un rafforzamento del ruolo della compliance nella valutazione preventiva dei modelli di outsourcing e nel controllo degli ecosistemi di fornitura.

Ultimo punto, ma non meno importante, la dimensione culturale della compliance. La conformità non può essere delegata alla sola funzione specialistica; deve diventare parte della cultura d'impresa, permeare le decisioni strategiche, l'operatività quotidiana e il modo di relazionarsi con il mercato. La maturità della compliance si manifesta quando il rispetto delle regole non è più avvertito come un'imposizione esterna, ma come un valore cardine dell'agire aziendale.

In conclusione, la compliance non rappresenta un costo da contenere o un ostacolo da aggirare, ma una infrastruttura essenziale di fiducia, sostenibilità e competitività. In una fase storica caratterizzata da innovazioni dirompenti, da forti interdipendenze e da normative sempre più impattanti e sofisticate, la qualità della funzione di conformità rappresenterà uno dei principali fattori distintivi delle organizzazioni e abiliterà l'impresa a gestire il cambiamento, diventando la funzione il luogo dove tale cambiamento viene studiato, compreso e orientato.

Il volume raccoglie gli atti del convegno Regolamentazione e innovazione. Compliance motore di sviluppo e sfida strategica per la crescita aziendale, organizzato dal Compliance Lab e da AICOM – Associazione Italiana Compliance presso il Dipartimento di Economia Aziendale dell'Università degli Studi di Roma Tre. L'iniziativa ha celebrato il ventennale della funzione compliance e ha riunito rappresentanti delle principali istituzioni di vigilanza nazionali e bancarie europee insieme a esponenti di primari gruppi finanziari italiani.

IL COMPLIANCE LAB

è un laboratorio di ricerca del Dipartimento di Economia Aziendale che si propone di promuovere la produzione e la diffusione di conoscenza sul tema della compliance in campo economico-manageriale.

Roma Tre