Pubblicazione Trimestrale
ISSN: 2279-9737

# Rivista di Diritto Bancario

dottrina
e giurisprudenza
commentata

Gennaio / Marzo
2026

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata



2026

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

# NORME PER LA VALUTAZIONE E LA PUBBLICAZIONE

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

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

I contributi sono anonimizzati prima dell'invio ai valutatori.

Le schede di valutazione sono inviate agli autori previa anonimizzazione.

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

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

Rivista di Diritto Bancario
dottrina e giurisprudenza commentata

**SEDE DELLA REDAZIONE**

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

CHIARA D'ELIA – FEDERICA CASAROSA

# *Cloud computing* e settore assicurativo. Profili giuridici dell'esternalizzazione tecnologica tra innovazione digitale e *compliance* multilivello



## 1. *Introduzione*

Nel quadro della trasformazione digitale che permea trasversalmente ogni settore dell'economia globale, il comparto assicurativo appare quale terreno privilegiato di sperimentazione e, al contempo, di tensione normativa, essendo chiamato a ripensare radicalmente le proprie infrastrutture operative, informative e relazionali. In tale contesto, il *cloud computing* si afferma non già quale mera innovazione strumentale, bensì come paradigma infrastrutturale idoneo a trasformare in modo radicale i processi di *back* e *front office* assicurativo, la gestione documentale, la conservazione dei dati e la continuità operativa delle funzioni critiche, determinando una progressiva esternalizzazione dei processi e sollevando questioni in materia di sicurezza informatica, *compliance* normativa e *governance* dei dati[1]. Siffatta delega di funzioni essenziali ad attori terzi introduce

This work was supported by the EU Horizon Europe Framework Program under Grant Agreement n° 101119547 (*PQ-REACT*).

[1] A. MANTELERO, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, in *Diritto dell'informazione e dell'informatica*, n. 4/2010, 673, nonché i diversi contributi contenuti in C. MILLARD (a cura di), *Cloud Computing Law*, 2ª ed., Oxford University Press, Oxford, 2021 (ed. *online*: Oxford Law Pro, 17 giugno 2021). In termini più ampi, la digitalizzazione mette progressivamente in tensione i modelli tradizionali di organizzazione e interazione, favorendo dinamiche di disintermediazione e decentramento, l'integrazione tra filiere e funzioni un tempo distinte, l'affermazione di nuovi soggetti

un dualismo intrinseco che segna la fisionomia stessa del fenomeno: da un lato, l'aspirazione all'efficienza gestionale, all'ottimizzazione dei costi e all'innovazione di processo; dall'altro, l'inderogabile necessità di assicurare la conformità alla cornice regolatoria, la salvaguardia della sicurezza informatica e la piena governabilità dei dati[2]. Se l'adozione di architetture *cloud* consente il conseguimento di vantaggi competitivi legati alla scalabilità elastica delle risorse computazionali e a una più elevata resilienza in termini di continuità operativa e sicurezza informatica[3] essa impone al contempo una profonda riconfigurazione del perimetro soggettivo delle responsabilità giuridiche[4], nonché una

attivi nella catena del valore e una trasformazione profonda del ruolo dell'utente. Quest'ultimo, infatti, non è più solo destinatario passivo di servizi digitali, ma partecipa attivamente alla loro generazione e configurazione, attraverso il costante rilascio di dati che ne influenzano struttura e contenuti, contribuendo così alla definizione dell'esperienza digitale stessa. Sul punto, cfr. V. FALCE – J. CANNATACI – O. POLLICINO, *Legal Challenges of Big Data, Cheltenham*, UK, 2020; V. FALCE – A. GENOVESE, *La portabilità dei dati in ambito finanziario*, *Quaderno FinTech*, CONSOB, 2021. Per un'analisi delle dinamiche che hanno condotto all'affermazione delle TechFin e delle peculiarità che le distinguono, si veda D.A. ZETZSCHE – R.P. BUCKLEY – D.W. ARNER – J.N. BARBERIS*, From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, *EBI Working Paper Series*, n. 6/2017.

[2] Sul punto si veda ANCHE P. LUCANTONI – C. VILLANI, *La gestione e supervisione dei rischi ICT e di sicurezza nelle attività finanziarie esternalizzate tra DORA e CRD VI*, in *Dialoghi di Diritto dell'Economia*, fasc. 1/2025, p. 1 ss.

[3] Sotto questo profilo si rimanda alla letteratura aziendalistica sul punto. Senza ambizione di esaustività, si segnalano: M. ARMBRUST ET AL., *A View of Cloud Computing*, in *Communications of the ACM*, vol. 53, n. 4/2010, 50-58; R.D. CHAKLADAR, *Leveraging Cloud Technology for Data and Analytics in the Insurance Industry*, in *International Journal of Core Engineering & Management*, vol. 7, n. 9/2024, disponibile online: https://ijcem.in; ENISA, *Cloud Computing: Benefits, Risks and Recommendations for Information Security*, 2012; N. MALALI, *Cloud-Native Security and Compliance in Life and Annuities Insurance: Challenges and Best Practices*, in *International Journal of Interdisciplinary Research Methods*, vol. 12, n. 1/2025, 50-73, disponibile online: https://eajournals.org; A. MARINOS – G. BRISCOE, *Community Cloud Computing*, in *Proceedings of the 1st International Conference on Cloud Computing (CloudCom)*, 2009; S. PEARSON, *Privacy, Security and Trust in Cloud Computing*, in *Privacy and Security for Cloud Computing,* Springer, 2013, 3-42; H.S. SCOTT – J. GULLIVER – H. NADLER, *Cloud Computing in the Financial Sector: A Global Perspective*, Program on International Financial Systems, 2019, disponibile online: https://ssrn.com/abstract=3427220.

[4] Sulle questioni relative alla dimensione contrattuale, si vedano: A. MANTELERO, *Il contratto per l'erogazione alle imprese di servizi di cloud computing (Cloud*

rivisitazione dei presìdi di vigilanza, dei meccanismi di *auditability* e delle modalità di esercizio dei poteri di controllo da parte delle autorità competenti, specie nei settori regolamentati e ad alta intensità di dati[5].

*Computing Contracts: B2B)*, Social Science Research Network, 30 maggio 2012, disponibile su: https://papers.ssrn.com/abstract=2142050, ultimo accesso 8 aprile 2026; W. KUAN HON – C. MILLARD, *Banking in the Cloud: Part 3 – Contractual Issues*, in *Computer Law & Security Review*, vol. 34/2018, 595 ss.; D. BOMHARD – A. DAUM, *Cybersecurity in Outsourcing and Cloud Computing: A Growing Challenge for Contract Drafting*, in *International Cybersecurity Law Review*, vol. 2/2021, 161 ss.; M. LIMONE, *I contratti di cloud*, in *Comparazione e diritto civile*, n. 1/2013. In materia di protezione dei dati personali, si vedano: W. KUAN HON – C. MILLARD – I. WALDEN, *The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated? – The Cloud of Unknowing*, in I*nternational Data Privacy Law*, vol. 1/2011, 211 ss.; ID., *Who Is Responsible for "Personal Data" in Cloud Computing? – The Cloud of Unknowing, Part 2*, in *International Data Privacy Law*, vol. 2/2012, 3 ss.; J. ABRERA, *Data Privacy and Security in Cloud Computing: A Comprehensive Review*, in *Journal of Computer Science and Information Technology*, 2023. Quanto al profilo internazional-privatistico, si rinvia a G.M. RUOTOLO, *Hey! You! Get Off My Cloud! Accesso autoritativo alle nuvole informatiche e diritto internazionale*, disponibile su: https://papers.ssrn.com/abstract=2386763, ultimo 23 settembre 2025; M. Forti, *Contratti di cloud computing: tra profili di diritto internazionale privato e tutela della riservatezza*, in P. IVALDI – S. CARREA (a cura di), *Lo spazio cibernetico: rapporti giuridici pubblici e privati nella dimensione nazionale e transfrontaliera*, Torino, 2018, 199-232.

[5] Come evidenzia G. DE DONNO*, Osservatoio AIDA*, in *Assicurazioni*, n. 1/2025, pp 235 ss., il Regolamento DORA si inserisce nel solco di un'evoluzione normativa che mira al rafforzamento sistemico dei presìdi di sicurezza informatica, mediante l'introduzione di obblighi ulteriori che vanno a incidere, in modo significativo, sulle dinamiche dell'esternalizzazione tecnologica, con particolare riferimento alla gestione delle piattaforme applicative e dei flussi informativi. Tali attività, divenute oramai elementi strutturali e non meramente accessori della catena del valore degli intermediari assicurativi, hanno contribuito ad amplificare l'esposizione a rischi di natura cibernetica, accrescendo la probabilità che si verifichino eventi pregiudizievoli idonei a compromettere la continuità operativa di funzioni critiche. In tale contesto si collocano le iniziative promosse da IVASS, che ha progressivamente intensificato la propria azione di presidio attraverso una combinazione di attività di sensibilizzazione, accessi ispettivi e verifiche tecniche avanzate, tra cui *penetration test* condotti da soggetti qualificati, volte a rafforzare, in chiave preventiva, la resilienza digitale delle imprese sottoposte a vigilanza. È in questa medesima direzione che si orienta l'impianto regolatorio delineato da DORA, il quale pone l'accento su una concezione estesa e proattiva della sorveglianza, intesa come funzione distinta e complementare rispetto alla vigilanza in senso stretto, la quale interviene *ex post* e in una prospettiva prevalentemente sanzionatoria. Si configura così un paradigma di supervisione più maturo, fondato non solo sul controllo formale, ma sulla costruzione di una capacità

Inoltre, nel quadro della progressiva digitalizzazione di tutti i settori pubblici e privati, assume particolare rilevanza anche l'intervento del legislatore italiano che già nel 2017, con il Piano Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019, approvato con D.P.C.M. del 31 maggio 2017, ha avviato un processo di razionalizzazione e ammodernamento delle infrastrutture informatiche della Pubblica Amministrazione, basato sul principio del "*cloud first*"[6].

Questo percorso verso l'utilizzo generalizzato del *cloud computing*, tuttavia, si muove di pari passo agli interventi legislativi finalizzati a salvaguardare la sicurezza informatica, includendo tutte le attività necessarie per proteggere le reti e i sistemi informativi, gli utenti di tali sistemi e le altre persone colpite dalle minacce informatiche, così come definito nell'art. 2(1) del c.d. *Cybersecurity Act*[7]. Tale approccio consente di individuare interventi sui soggetti, sui processi e sulle tecnologie che possono operare nei diversi settori coinvolti. In tale prospettiva, l'ordinamento ha progressivamente strutturato un complesso quadro regolatorio multilivello, ispirato a criteri di integrazione e specializzazione, il cui fulcro si articola, in una prospettiva orizzontale e trasversale ai settori economici, attorno alla Direttiva (UE) 2022/2555 (c.d. *NIS* 2)[8], relativa alla sicurezza delle reti e dei sistemi informativi. Ad essa, si aggiungono poi gli obblighi

strutturale di resistenza agli *shock* digitali, quale condizione imprescindibile per la tutela dell'interesse pubblico e della stabilità del sistema assicurativo. Sul tema si veda anche W.R.M. LONG – L. CUYVERS – J. QUARTILHO, *New EU Cyber Law for the Financial Services Industry with Significant Impact on ICT Service Providers*, Sidley, 2023.

[6] E. MONTAGNANI, *Le pubbliche amministrazioni nell'era delle tecnologie cloud ed edge computing tra opportunità e rischi: il Piano Nazionale di Ripresa e Resilienza e la comunità digitali*, in *Rivista italiana di informatica e diritto*, n. 1/2022, 189.

[7] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

[8] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

previsti dal Regolamento (UE) 2016/679 (c.d. *GDPR*)[9], in materia di protezione dei dati personali, anch'essi applicabili a livello orizzontale.

Sul versante settoriale, il Regolamento (UE) 2022/2554 (c.d. *DORA*)[10] relativo alla resilienza operativa digitale per il settore finanziario introduce un *corpus* normativo specificamente calibrato sulle peculiarità del settore finanziario, delineando obblighi stringenti in materia di gestione del rischio informatico, resilienza digitale e *governance* tecnologica delle imprese assicurative[11]. Nel comparto assicurativo, emerge chiaramente una specificità della sicurezza informatica, che appunto trascende la dimensione meramente tecnica per assumere la natura di presidio giuridico a carattere sistemico[12], in

[9] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[10] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011. In tema si vedano diversi contributi che approfondiscono le principali linee evolutive e criticità applicative della disciplina. Fra tutti, I. GIRARDI, in *Il Regolamento sulla resilienza operativa digitale ("DORA"): obiettivi, disciplina e alcune sfide aperte*, in *Quaderni AMF Italia*, n. 2/2024, 18 ss.; D. CLAUSMEIER, *Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)*, in *International Cybersecurity Law Review*, 2023, 79 ss.

[11] V. N. MICHIELI, in *Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance*, in *Banca impresa società*, 2024, 252 ss., che riflette sul rilievo che la nuova disciplina assume nella definizione degli assetti di governo societario, specie in relazione alla gestione strategica dei rischi digitali.

[12] Come evidenziato da L. JANČIŪTĖ, *Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework*, in *International Cybersecurity Law Review*, (2025) 6, 146, il concetto di *rischio sistemico* è generalmente inteso come il rischio che si verifichi un'interruzione significativa del funzionamento del sistema finanziario, tale da produrre effetti negativi rilevanti sull'economia reale e sull'integrità del mercato interno. In questo senso, la stabilità finanziaria presuppone la capacità dei mercati di continuare a svolgere le proprie funzioni essenziali, quali l'intermediazione creditizia, la gestione dei pagamenti e la trasformazione delle scadenze, anche in presenza di *shock* esogeni o endogeni. Tale stabilità è compromessa quando il sistema non è in grado di assorbire tali *shock*, generando dinamiche amplificative che possono assumere la forma di *bank run*, crisi di liquidità, blocchi nell'erogazione del credito, vendite forzate di attivi, crolli di mercato o

quanto funzionale alla salvaguardia di interessi pubblici primari quali la stabilità dell'ordinamento finanziario e la preservazione della fiducia collettiva nei mercati[13].

Il presente contributo si propone, dunque, di esaminare le problematiche giuridiche che emergono dall'interazione tra *cloud computing* e disciplina sulla sicurezza informatica applicabile agli operatori assicurativi, muovendo da una ricostruzione del quadro normativo multilivello e analizzando le principali incertezze interpretative e applicative[14]. L'obiettivo è duplice: da un lato, chiarire il perimetro degli obblighi cui sono soggette le istituzioni finanziarie che ricorrono a servizi *cloud*, con particolare attenzione alle sovrapposizioni e alle frizioni tra regimi normativi concorrenti; dall'altro, indagare se e in quale misura l'adozione di standard tecnici, nazionali, europei o internazionali, possa essere considerata condizione

fenomeni di iperinflazione. In questa prospettiva, il rafforzamento della resilienza operativa si configura come uno strumento funzionale non solo alla continuità aziendale del singolo operatore, ma alla tenuta sistemica dell'intero ecosistema finanziario. V. in questo senso EUROPEAN SYSTEMIC RISK BOARD, *Cyber Systemic Risk*, febbraio 2020, L. KAFFENBERGER – E. KOPP, *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment*, Carnegie Endowment for International Peace, 2019.

[13] Sul tema, v. D. CLAUSMAIER, *Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)*, in *International Cybersecurity Law Review*, 2023, IV, 80 ss.; S. KOURMPETIS, *Management of ICT Third Party Risk under the Digital Operational Resilience Act*, in L. BÖFFEL – J. SCHÜRGER (a cura di), *Digitalisation, Sustainability, and the Banking and Capital Markets Union*, EBI Studies in Banking and Capital Markets Law, Palgrave Macmillan, Cham, 2023, disponibile all'indirizzo: https://doi-org.ezp.biblio.unitn.it/10.1007/978-3-031-17077-5_7; E. KUN, *From Operational Risk to Systemic Risk: The EU's Digital Operational Resilience Act for Financial Services (DORA)*, 2021, disponibile su: https://www.law.kuleuven.be/citip/blog/from-operational-risk-to-systemic-risk/, ultimo accesso 8 aprile 2026.

[14] L'attenzione di regolatori, autorità di vigilanza e organismi sovranazionali nei confronti dei rischi cibernetici nel settore finanziario non rappresenta una novità recente, ma si inserisce in un percorso di consapevolezza progressiva sviluppatosi nell'ultimo decennio. Le minacce legate alla sicurezza informatica, specie in relazione ai servizi bancari digitali, sono state oggetto di crescente attenzione, anche in ambito scientifico. Per una ricostruzione sistematica e storica dell'evoluzione di tali rischi, si veda A.T. OYEWOLE – C.C. OKOYE – O.C. OFODILE – C.E. UGOCHUKWU, *Cybersecurity Risks in Online Banking: A Detailed Review and Preventing Strategies Application*, in *World Journal of Advanced Research and Reviews*, 2024, 627 ss.

sufficiente per garantire la *compliance* alle normative vigenti, o se non si imponga piuttosto una nozione più esigente di conformità sostanziale, capace di integrare prescrizione normativa, *governance* tecnologica e responsabilità organizzativa in un sistema coerente e continuamente adattivo.

Particolare attenzione sarà rivolta ai profili di interazione tra discipline di fonte e natura diversa citati sopra: la normativa generale in materia di *cybersecurity* (*NIS* 2 e la relativa normativa di implementazione)[15], quella specifica per il settore assicurativo (*DORA*), le disposizioni in materia di protezione dei dati personali (*GDPR*), nonché agli schemi di certificazione e standardizzazione promossi dall'ISO (*International Organization for Standardization*), dall'*ENISA* (*European Union Agency for Cybersecurity*) e dal *NIST* (*National Institute of Standards and Technology*). Tale pluralismo normativo solleva interrogativi circa la reciproca integrazione, la coerenza sistemica e l'effettiva applicabilità da parte degli operatori assicurativi, specie quelli di dimensioni medio-piccole[16].

L'approccio metodologico adottato deve necessariamente essere di tipo interdisciplinare[17]: accanto all'analisi giuridica delle fonti, si farà

[15] Decreto legislativo 4 settembre 2024, n. 138 – Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

[16] Sul punto, G. DE DONNO, *op. cit.,* 241, riportando l'intervento del dott. Pietro Ranieri, responsabile *Compliance and Group Anti-Money Laundering* di Unipol Assicurazioni, nell'ambito del convegno *"La vigilanza del mercato assicurativo di fronte all'evoluzione tecnologica e al principio di sostenibilità"*, svoltosi a Firenze il 7 febbraio 2025, osserva come il quadro regolatorio multilivello elaborato a livello unionale determini pressioni rilevanti sulle imprese assicurative, in particolare su quelle di minori dimensioni, che si trovano a dover sostenere obblighi di conformità spesso sproporzionati rispetto alle risorse disponibili. Al contempo, anche gli operatori più strutturati rischiano di vedere limitata la propria capacità di innovazione, in ragione di vincoli normativi eccessivamente analitici, che impongono requisiti puntuali la cui attuazione può generare un sovraccarico procedurale non sempre funzionale alla realizzazione degli obiettivi sostanziali di tutela cui la regolazione è preordinata. In tale prospettiva, è stato opportunamente osservato che la disciplina di settore dovrebbe evitare di limitare oltre il necessario le possibilità di sperimentazione e adattamento delle imprese, poiché ciò finisce per incidere negativamente sulla dinamica concorrenziale e, in ultima analisi, sul benessere del consumatore.

[17] Lo rilevano C.P. BUTTIGIEG – B.B. ZIMMERMANN, *The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's*

riferimento alle prassi operative, alle linee guida emanate dalle autorità di vigilanza e ai documenti di standardizzazione allo scopo di offrire un quadro il più possibile completo e operativo per gli interpreti del diritto e per i responsabili della *governance* digitale nelle imprese assicurative.

La complessità del tema risiede a ben vedere non solo nella molteplicità delle fonti coinvolte, ma anche nella rapidità con cui le tecnologie evolvono e si diffondono, talvolta superando la capacità del legislatore di approntare risposte regolatorie adeguate. Di qui la necessità di interrogarsi circa l'idoneità dell'impianto normativo tradizionale, imperniato su una regolazione di tipo verticale, a garantire un livello di tutela adeguato nell'attuale ecosistema digitale, caratterizzato da incessanti mutamenti tecnologici e da una crescente interconnessione sistemica. Si fa infatti sempre più strada l'esigenza di un modello regolatorio alternativo, ispirato a una logica maggiormente flessibile e adattiva, fondato su principi generali, standard[18] e meccanismi di *accountability*, idonei a coniugare certezza giuridica, nonché a rafforzare la responsabilizzazione degli attori coinvolti.

*Architecture for Financial Supervision*, in *ERA Forum*, vol. 25/2024, 11-28, disponibile su https://doi.org/10.1007/s12027-024-00793-w. In prospettiva sistemica, si ricorda che *"Fintech" is an umbrella term encompassing a wide variety of business models*, come evidenziato dalla BANCA CENTRALE EUROPEA, *Guide to Assessments of Fintech Credit Institution Licence Applications*, settembre 2017, disponibile all'indirizzo https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.201803_guide_assessment_fintech_credit_inst_licensing.en.pdf (ultimo accesso 8 aprile 2026). In questo senso anche V. FALCE, *Data strategy e finanza digitale. Il caso della "consulenza automatizzata"*, in *Assicurazioni*, n. 4/2022, 431.

[18] Secondo la definizione contenuta nella ISO/IEC Guide 2:2004, n. 3.2, uno standard è qualificabile come un «documento, elaborato attraverso un processo consensuale e approvato da un organismo riconosciuto, che stabilisce, per applicazione comune e reiterata, regole, linee guida o specifiche tecniche concernenti attività o i relativi risultati, con l'obiettivo di perseguire il livello ottimale di ordine all'interno di un determinato contesto». Inoltre, si precisa che «gli standard dovrebbero fondarsi su risultati consolidati della scienza, della tecnologia e dell'esperienza pratica, e perseguire la finalità di promuovere il massimo beneficio per la collettività».

## 2. *Il ruolo del cloud computing nel mercato assicurativo*

L'evoluzione tecnologica che ha interessato il settore assicurativo, e finanziario nel suo complesso, negli ultimi due decenni ha comportato un profondo mutamento, come si è detto, nei modelli organizzativi e nelle strategie operative delle imprese assicurative[19].

Tra le tecnologie abilitanti che hanno maggiormente influenzato tale trasformazione, il *cloud computing* occupa una posizione di primo piano[20]. Trattasi, invero, di un modello architetturale innovativo fondato sull'erogazione, per il tramite della rete Internet, di risorse informatiche quali potenza computazionale, capacità di archiviazione e strumenti applicativi, configurati come servizi *on demand* accessibili da remoto[21]. Questo modello consente una dematerializzazione delle

[19] Cfr., *ex multis*, R. BASKERVILLE – F. CAPRIGLIONE – N. CASALINO, *Impacts, Challenges and Trends of Digital Transformation in the Banking Sector*, in *Law and Economics Yearly Review*, 2020, 341 ss.

[20] Si veda W. KUAN HON – C. MILLARD, *Banking in the Cloud: Part 1 – Banks' Use of Cloud Services*, in *Computer Law & Security Review*, vol. 34/2018, 4 ss. Si veda altresì il report elaborato per l'anno 2023 dalla CLOUD SECURITY ALLIANCE (CSA), dal quale emerge con chiarezza il radicamento pervasivo dei servizi *cloud* in tutte le componenti operative e strategiche del settore finanziario: *State of Financial Services in Cloud Report*, 2023, disponibile all'indirizzo https://cloudsecurityalliance.org/artifacts/state-of-financial-services-in-cloud (ultimo accesso 8 aprile 2026).

[21] Per quanto la terminologia di *cloud computing* sia presente nei testi legislativi europei più recenti, non esiste una definizione giuridica di *cloud computing*. La definizione più aggiornata è quella offerta dallo Standard ISO/IEC 22123-1:2023(E) – *Information technology – Cloud computing – Part 1: Vocabulary* (2023), in cui appunto il *cloud computing* è definito come "un paradigma per consentire l'accesso di rete a un *pool* scalabile ed elastico di risorse fisiche o virtuali condivisibili con provisioning *self-service* e amministrazione su richiesta". Sempre fra le definizioni di natura tecnica, è utile menzionare quella fornita dal *National Institute of Standards and Technology* (*NIST*), secondo cui il *cloud computing* è un modello che consente, attraverso la rete Internet, l'accesso pervasivo, comodo e su richiesta a un insieme condiviso di risorse informatiche configurabili, quali reti, server, sistemi di archiviazione, applicazioni e servizi, gestite da terze parti. In tale prospettiva, l'utente può utilizzare spazi di memorizzazione, ambienti di sviluppo o *software* applicativi senza che le relative risorse risiedano fisicamente nei propri sistemi informatici, bensì mediante connessioni a *server* remoti esterni, gestiti all'interno di infrastrutture centralizzate. Il *NIST* individua altresì cinque caratteristiche essenziali di tale paradigma: *self-service* su richiesta, ampio accesso alla rete, condivisione delle risorse, rapidità di elasticità e servizio misurabile, che definiscono la natura dinamica,

infrastrutture fisiche tradizionalmente adibite all'elaborazione e alla conservazione dei dati, determinando un mutamento strutturale e sistemico nell'assetto organizzativo dei processi informatici e gestionali[22]. Ciò avviene in ragione della possibilità, insita nelle architetture *cloud*, di accedere a risorse computazionali e di archiviazione digitali secondo modalità scalabili, flessibili e modulari, senza vincoli spaziali o temporali, mediante la loro allocazione su *server* virtualizzati localizzati presso *data center* territorialmente distribuiti, anche al di fuori del perimetro giurisdizionale nazionale[23].

Sul piano giuridico, ciò comporta a ben vedere rilevanti implicazioni in ordine alla *governance* dei dati, alla tutela della riservatezza, alla localizzazione giurisdizionale delle informazioni nonché alla definizione delle responsabilità contrattuali ed extracontrattuali tra i soggetti coinvolti nella fornitura e nella fruizione dei servizi *cloud*.

Il *cloud computing* si articola in una pluralità di modelli di servizio, i quali si differenziano in base al livello di gestione delegata delle risorse tecnologiche: quanto più ampio è lo strato di infrastruttura

scalabile e standardizzata del *cloud computing*. Si veda P. MELL – T. GRANCE, "*The NIST Definition of Cloud Computing*", 2011, https://csrc.nist.gov/publications/detail/sp/800-145/final e A. MANTELERO, *Il contratto per l'erogazione alle imprese di servizi di cloud computing*, in *Contr. impr*., 2012, 1216. V. anche EIOPA, *Orientamenti in materia di esternalizzazione a fornitori di servizi cloud*, EIOPA-BoS-20-002, 6 febbraio 2020 che per «servizi *cloud*» intende "servizi forniti tramite *cloud computing*, ossia un modello che consente l'accesso in rete diffuso, pratico e su richiesta a un gruppo condiviso di risorse elettroniche configurabili (ad esempio, reti, *server*, memorie, applicazioni e servizi), che possono essere forniti e messi a disposizione rapidamente con un minimo di impegno gestionale o di interazione con il fornitore del servizio".

[22] Come rilevato da R. NAYDENOV – D. LIVERI – L. DUPRE – E. CHALVATZI, *Secure Use of Cloud Computing in the Finance Sector – Good practices and recommendations*, dicembre 2015, disponibile sul sito istituzionale di ENISA, 20, tra le principali motivazioni che spingono verso l'adozione di soluzioni *cloud* vi sono la riduzione del *Total Cost of Ownership*, il minor tempo necessario per il provisioning dei servizi, la rapidità di accesso al mercato e la flessibilità sia infrastrutturale che economica. Le autorità nazionali di vigilanza finanziaria considerano, inoltre, la *business continuity* come uno degli incentivi più rilevanti all'adozione di servizi *cloud*.

[23] Tale dislocazione transfrontaliera delle risorse solleva, peraltro, rilevanti questioni in punto di giurisdizione, applicabilità della normativa interna e garanzie di conformità ai presìdi di sicurezza, riservatezza e integrità dei dati imposti dall'ordinamento. Si veda sul punto W. KUAN HON – C. MILLARD, *op. cit.,* 595 ss.

informatica affidato al *provider* (fornitore del servizio), tanto maggiore è il grado di semplificazione per il cliente (utilizzatore finale), che viene progressivamente sollevato dalla cura delle componenti *hardware* e *software* sottostanti[24]. In particolare, si individuano le seguenti principali categorie:

- *Infrastructure as a Service* (*IaaS*), rappresenta un modello di servizio *cloud* in cui le risorse informatiche accessibili tramite rete, quali capacità di calcolo (*compute*), spazio di archiviazione (*storage*) e connettività di rete (*networking*), vengono fornite in modalità virtualizzata dal *cloud provider*. Qui il fornitore gestisce e mantiene l'infrastruttura fisica sottostante, mentre permane in capo all'utente finale la responsabilità della gestione dei server virtuali (*virtual machines*), ivi inclusi i sistemi operativi, i *middleware*, le applicazioni installate e i relativi dati[25]. Nel settore assicurativo, tali servizi trovano applicazione, ad esempio, nell'implementazione di ambienti ad alte prestazioni destinati all'elaborazione di modelli attuariali complessi, alla simulazione di scenari previsionali di rischio, o al calcolo di indicatori di solvibilità dinamica. In questi casi, l'impresa conserva il controllo sull'intero *stack software*, beneficiando al contempo della scalabilità, dell'affidabilità e della disponibilità garantite dall'infrastruttura del fornitore.

- *Platform as a Service* (*PaaS*), si caratterizza per la fornitura, da parte del *cloud provider*, di un ambiente integrato per lo sviluppo, il *testing*, l'*hosting* e la distribuzione di applicazioni *software*, il cui codice sorgente viene caricato direttamente dal cliente. Questo modello esonera l'utilizzatore dall'onere di amministrare l'infrastruttura fisica e logica sottostante (*server*, sistemi operativi, *middleware*, *database*), consentendogli di concentrare le risorse sulla programmazione e

[24] D. GERADIN ET AL., *The Regulation of Cloud Computing: Getting It Right*, in *SSRN Electronic Journal*, 2022, disponibile su: https://www.ssrn.com/abstract=4285731, ultimo accesso 8 aprile 2026. Vedasi anche ENISA, *Cloud cybersecurity market analysis*, marzo 2023, disponibile sul sito istituzionale, 18 ss.

[25] Tra i principali servizi IaaS si annoverano *Amazon EC2, Amazon S3, Route 53, Google Compute Engine (parte della Google Cloud Platform), IBM SoftLayer* e *Microsoft Azure. Cfr.* W. KUAN HON – C. MILLARD, *Banking in the Cloud: Part 1 – Banks' Use of Cloud Services*, cit., 5.

sull'ottimizzazione delle funzionalità applicative[26]. In ambito assicurativo, ambienti *PaaS* vengono spesso impiegati per sviluppare soluzioni applicative personalizzate, ad esempio per la gestione dinamica dei preventivi, integrati con i sistemi *core* attraverso API sicure. Questo approccio consente alle imprese di focalizzarsi sulle attività a maggior valore aggiunto delegando al *provider* la gestione della piattaforma tecnologica sottostante, con benefici in termini di efficienza, scalabilità e velocità di rilascio[27].

- *Software as a Service* (*SaaS*), che rappresenta un modello di servizio "chiavi in mano", mediante il quale l'utente accede, tipicamente via *browser*, a *software* applicativi completamente gestiti dal fornitore, senza necessità di installazione o manutenzione locale. Nel contesto assicurativo, esempi di adozione del modello *SaaS* includono piattaforme come *Salesforce Financial Services Cloud*, impiegate per la gestione integrata delle relazioni con il cliente, o soluzioni di firma elettronica come *DocuSign*, funzionali alla digitalizzazione dei processi di sottoscrizione contrattuale.

Il passaggio da *IaaS* a *SaaS* non comporta soltanto un incremento della semplificazione operativa, ma ridisegna progressivamente l'allocazione delle responsabilità giuridiche tra impresa assicurativa e *provider*, con implicazioni dirette sulla qualificazione dei ruoli soggettivi ai sensi del GDPR, sulle clausole contrattuali necessarie e sull'ampiezza dei poteri di audit esercitabili dall'impresa.

Ciascuna delle modalità architetturali adottabili in ambito *cloud*, sia essa riconducibile a modelli di tipo *IaaS*, *PaaS* o *SaaS*, implica differenti assetti contrattuali e conformazioni operative, dando origine a un sistema complesso di allocazione e gestione condivisa del rischio. In tale contesto, le obbligazioni afferenti alla custodia, alla sicurezza, all'integrità e alla disponibilità dei dati si distribuiscono secondo logiche variabili, in funzione del modello tecnologico e gestionale prescelto, rendendo imprescindibile una meticolosa definizione delle clausole contrattuali. Particolare rilievo assumono, in tal senso, le pattuizioni in materia di riparto delle responsabilità, livelli minimi di

[26] Esempi di servizi *PaaS* includono *Google App Engine* (parte della *Google Cloud Platform*), *IBM Bluemix* (basato su *SoftLayer*), e *Azure App Services* di *Microsoft.* IBID.

[27] Cfr. E. SIMMON, *Evaluation of Cloud Computing Services Based on NIST SP 800-145*, in *NIST Special Publication 500-322*, febbraio 2018, 8-11.

servizio (*Service Level Agreements – SLA*[28]), misure di protezione dei dati personali, continuità operativa e *disaster recovery*, le quali devono essere formulate in modo da garantire la conformità agli obblighi imposti dall'ordinamento, nonché da assicurare un adeguato bilanciamento tra le esigenze dell'ente assicurativo e le prerogative del fornitore di servizi.

Sotto il profilo della distribuzione e dell'architettura del servizio, si distinguono invece quattro modelli principali:

- il *cloud pubblico*, nel quale le risorse computazionali (*server*, *storage*, potenza elaborativa) sono messe a disposizione di una pluralità indifferenziata di utenti su infrastrutture di proprietà e sotto il controllo esclusivo del fornitore del servizio. Nel contesto assicurativo, il *cloud* pubblico viene frequentemente impiegato per l'erogazione di servizi a bassa criticità, quali la gestione delle campagne *marketing* digitali, la reportistica non sensibile o i sistemi di *front-end* per il calcolo dei preventivi *online*[29].

- il *cloud privato* è un modello di distribuzione *cloud* riservato a un singolo soggetto giuridico, configurato per garantire il massimo grado di controllo e personalizzazione delle risorse digitali. Tale architettura può essere ospitata "*on-premise*", ovvero presso le infrastrutture fisiche dell'organizzazione cliente, dove può essere gestita direttamente dall'impresa, oppure "*off-premise*", presso un *data center* esterno gestito da un fornitore terzo, incaricato della creazione, gestione e manutenzione dell'ambiente *cloud*. Quest'ultima configurazione si

---

[28] K. STYLIANOU – J. VENTURINI – N. ZINGALES, *Protecting user privacy in the Cloud: an analysis of terms of serivce*, in *Eur. Jour. Law and Technology*, 2015, 1. V. anche C. A. ROHRMANN – J. FALCI SOUSA ROCHA CUNHA, *Some Legal Aspects of Cloud Computing Contracts*, in *10 J. Int't Com. L. & Tech.*, 37, 2015, 41. Nel contesto delle iniziative europee volte a promuovere la trasparenza e l'affidabilità contrattuale nei rapporti tra fornitori e utilizzatori di servizi *cloud*, merita menzione il report identificato con codice SMART 2013/0039, *Standard Terms and Performance Criteria in Service Level Agreements for Cloud Computing* (*Contract n. 30-CE-0600116/00-34*). In tale documento, si evidenzia come il modello di *SLA* proposto debba essere inteso non quale strumento isolato, ma piuttosto come parte integrante di un quadro regolatorio europeo in evoluzione, in grado di coordinarsi e integrarsi con ulteriori iniziative parallele ancora in corso, quali i lavori del *Cloud Select Industry Group (C-SIG*) sul Codice di Condotta, i progetti relativi alla certificazione *cloud* e agli *SLA*, nonché l'elenco dei *Cloud Certification Schemespubblicato* da ENISA.

[29] IBID, 12-17.

avvicina, per natura giuridica e struttura operativa, a forme classiche di outsourcing dedicato[30]. Nel settore assicurativo, il *cloud* privato rappresenta una soluzione preferenziale per l'allocazione di applicazioni e dati particolarmente sensibili o strategici. Esso viene frequentemente impiegato per la gestione dei sistemi centrali di *back office*, delle piattaforme di sottoscrizione e liquidazione sinistri, nonché per l'archiviazione di dati sanitari o di informazioni rilevanti ai fini dell'adeguata verifica nell'ambito degli obblighi previsti dalla disciplina antiriciclaggio (*AML*). In simili contesti, l'isolamento fisico e/o logico delle risorse consente di assicurare livelli più elevati di riservatezza, integrità e conformità normativa, ponendosi in linea con i presidi richiesti dal legislatore e dalle autorità di vigilanza. In aggiunta agli obblighi derivanti dai diversi plessi normativi europei, analizzati nel prosieguo, si aggiungono i vincoli derivanti dalla disciplina nazionale antiriciclaggio (D.lgs. 231/2007), che all'art. 31, come modificato dal D.lgs. 125/2019, prescrive l'obbligo di adottare sistemi di conservazione sicuri, accessibili e tracciabili delle informazioni acquisite ai fini dell'adeguata verifica della clientela. In questa cornice, anche gli *Orientamenti EIOPA* in materia di *outsourcing* a fornitori *cloud* e le disposizioni dell'IVASS – in particolare il Regolamento n. 38/2018, artt. 30-32, relativi al sistema di governo societario e alle esternalizzazioni di funzioni essenziali o importanti – ribadiscono la centralità di soluzioni infrastrutturali che assicurino auditabilità, disponibilità e trasparenza nei rapporti con i fornitori esterni, ponendo il presidio contrattuale e organizzativo come condizione imprescindibile della digitalizzazione del settore assicurativo.

- il *cloud ibrido* rappresenta una configurazione mista che combina componenti di *cloud* pubblico e *cloud* privato all'interno di un ecosistema tecnologico interoperabile, con l'obiettivo di bilanciare efficienza operativa, flessibilità e tutela della riservatezza. Questo modello può concretizzarsi, ad esempio, attraverso il mantenimento di

[30] In un contesto *on-premise*, il *cloud* privato può essere implementato mediante piattaforme *IaaS/PaaS* come *VMware vSphere, IBM Softlayer/Bluemix* o *Microsoft Azure*, installate localmente. Analogamente, *software* per la raccolta, il monitoraggio e l'analisi dei dati, come *Splunk*, frequentemente adottato da istituzioni finanziarie europee, può essere utilizzato sia in modalità *SaaS* sia come installazione interna. W. KUAN HON – C. MILLARD, *Banking in the Cloud: Part 1 – Banks' Use of Cloud Services*, cit., 6.

particolari categorie di dati o delle funzioni critiche all'interno di ambienti privati o *on-premise*, mentre l'elaborazione di dati non sensibili o l'erogazione di servizi a bassa criticità avviene in ambiente pubblico. Nel settore assicurativo, il modello ibrido è particolarmente adatto per soluzioni architetturali modulari: ad esempio, una compagnia può impiegare un *cloud* privato per la gestione dei sinistri e dei contratti assicurativi, riservando invece l'uso del *cloud* pubblico a operazioni di *business intelligence* su *dataset* anonimizzati o all'erogazione di servizi digitali e mobile alla clientela *retail*. Tale ripartizione risponde non solo a esigenze di efficienza gestionale, ma anche ai vincoli imposti dal quadro regolatorio europeo.

- il modello *multi-cloud*, che prevede l'utilizzo simultaneo e coordinato di servizi offerti da più *provider*, con l'obiettivo di diversificare il rischio di dipendenza da un singolo fornitore (*vendor lock-in)*, migliorare la resilienza e ottimizzare le prestazioni. Nel contesto assicurativo, è crescente l'adozione di architetture *multi-cloud* da parte di gruppi internazionali che operano in più giurisdizioni, i quali si avvalgono di *cloud provider* differenti per garantire la compliance con le normative locali (es. *data residency*) e la continuità operativa *cross-border*[31]. Il ricorso a più fornitori, tuttavia, non si traduce soltanto in una scelta di efficienza tecnica, ma risponde a precisi obblighi regolatori. In tale prospettiva, il modello *multi-cloud* rappresenta, dunque, per le imprese assicurative non solo una forma di tutela contro l'obsolescenza tecnologica e le interruzioni di servizio, ma anche uno strumento di *compliance* avanzata, idoneo ad armonizzare le esigenze operative con i vincoli normativi imposti dalla molteplicità di ordinamenti in cui esse operano.

Avendo riguardo al settore assicurativo, il ricorso al *cloud computing* non si esaurisce in un mero strumento di supporto informatico, bensì si configura quale leva strategica di trasformazione dell'impresa assicurativa, capace di abilitare nuovi modelli di servizio, potenziare l'analisi predittiva dei rischi e ottimizzare la gestione dei

[31] V. EIOPA, *The Future of Cloud Computing and AI in the EU Insurance Sector*, 11 settembre 2024, disponibile all'indirizzo https://www.eiopa.europa.eu/publications/future-cloud-computing-and-ai-eu-insurance-sector_en.

sinistri[32]. L'adozione di soluzioni *cloud* da parte degli operatori del settore assicurativo assume, infatti, un ruolo determinante per il conseguimento di una maggiore agilità operativa, la razionalizzazione dei costi connessi alla gestione delle infrastrutture informatiche tradizionali, nonché per l'abilitazione di una scalabilità dinamica delle risorse tecnologiche, coerente con l'evoluzione dei fabbisogni aziendali. A ciò si aggiunge il potenziamento della resilienza operativa, intesa quale capacità dell'impresa di assicurare la continuità e l'affidabilità dei processi anche in presenza di eventi avversi[33].

Tali benefici trovano puntuale rispondenza nei princìpi delineati dalle *Guidelines on outsourcing to cloud service providers* emanate da EIOPA[34], le quali ribadiscono la necessità di garantire trasparenza,

[32] Cfr. J. WUERMELING, *Exploring DORA – The Digital Operational Resilience Act and its impact on banks and their supervisors*, in *SUERF Policy Briefs*, n. 210, ottobre 2021, 3; M. ELING – M. LEHMANN, *The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks*, in *The Geneva Papers on Risk and Insurance* – Issues and Practice, vol. 43, n. 3/2018, 359-396; R. DEB CHAKLADAR, *op. cit.*, 12-18.

[33] BASEL COMMITTEE ON BANKING SUPERVISION, *Principles for operational Resilience*, marzo 2021, disponibile alla pagina https://www.bis.org/bcbs/publ/d516.pdf, 2, che definisce la «*resilienza operativa*» come la capacità dell'intermediario bancario di garantire l'erogazione delle funzioni critiche anche in presenza di eventi dirompenti. Tale capacità si sostanzia nella predisposizione di misure che consentano all'ente di identificare e proteggersi da minacce e vulnerabilità operative, di rispondere e adattarsi a eventi perturbativi, nonché di ripristinare la continuità operativa e trarre insegnamento dalle disfunzioni registrate, al fine di minimizzarne l'impatto sull'erogazione dei servizi essenziali. In quest'ottica, l'intermediario deve adottare una logica *ex ante*, assumendo come presupposto la non eccezionalità del rischio di interruzione e modellando i propri assetti di governo sulla base della propensione al rischio e della tolleranza alla discontinuità operativa.

[34] EIOPA, *Guidelines on outsourcing to cloud service providers*, 6 febbraio 2020, disponibili sul sito istituzionale all'indirizzo https://www.eiopa.europa.eu/publications/guidelines-outsourcing-cloud-service-providers_en. Le Linee guida mirano a promuovere la convergenza tra le pratiche di vigilanza dei diversi Stati membri e a offrire ai soggetti vigilati, in particolare alle imprese assicurative, indicazioni chiare e coerenti in ordine alle modalità di esternalizzazione dei servizi informatici critici su infrastrutture *cloud*. In particolare, EIOPA sottolinea come i servizi *cloud*, configurati secondo i modelli *SaaS*, *PaaS* e *IaaS*, comportino una combinazione di dimensioni tecniche e organizzative che devono essere adeguatamente presidiate sul piano contrattuale, operativo e di *governance*. Sul tema si consideri inoltre il *FinTech Action Plan* adottato dalla

tracciabilità e controllo nei rapporti con i fornitori esterni, e si inseriscono in un più ampio quadro regolatorio in materia di gestione dei rischi informatici e operativi[35]. A livello unionale, assumono rilievo le disposizioni della Direttiva 2009/138/CE (*Solvency II*), che, unitamente agli Orientamenti EIOPA in tema di sistema di governo societario, richiedono alle imprese assicurative l'adozione di assetti organizzativi e contrattuali idonei ad assicurare la continuità delle funzioni critiche e la piena governabilità delle esternalizzazioni. Tale impianto è stato ulteriormente rafforzato dal *DORA*, che introduce obblighi specifici di gestione dei rischi *ICT*, imponendo presidi di monitoraggio continuo, piani di *exit strategy* e misure di resilienza operativa anche in relazione a fornitori terzi di servizi *cloud*. A ciò si aggiungono, in via orizzontale, gli obblighi sanciti *GDPR*, che esige che le misure tecniche ed organizzative garantiscano, anche nei casi di *outsourcing*, riservatezza, integrità e disponibilità dei dati personali trattati[36].

---

Commisione europea nel 2018 (COMMISSIONE EUROPEA, COM(2018) 109 final, *Piano d'azione per la tecnologia finanziaria: per un settore dei servizi finanziari più competitivo e innovativo*), un documento strategico finalizzato a sostenere l'innovazione tecnologica nel settore finanziario europeo, garantendo al contempo la stabilità del sistema e la tutela degli utenti. Tra le 23 azioni previste, il Piano sollecita in modo esplicito le autorità europee di vigilanza, tra cui EIOPA, a valutare la necessità di chiarimenti normativi in merito all'impiego di tecnologie emergenti, tra cui il *cloud computing*, allo scopo di evitare incertezze interpretative e rischi di arbitraggio regolamentare.

[35] Le Linee guida sull'esternalizzazione dei servizi informatici critici a fornitori *cloud* hanno l'obiettivo di delineare un quadro operativo e prudenziale per l'impiego responsabile e conforme di tali soluzioni da parte delle imprese assicurative. Le autorità di vigilanza europee sono sempre più consapevoli del crescente ricorso, da parte degli operatori finanziari, all'adozione di servizi basati su architetture *cloud*, o della concreta intenzione di ricorrervi. Dal punto di vista delle autorità nazionali di vigilanza, risulta prioritario inquadrare correttamente, anche sotto il profilo prudenziale, la disciplina normativa primaria e secondaria applicabile ai servizi *cloud*. In linea generale, tali servizi vengono qualificati dalle autorità di vigilanza come una forma di esternalizzazione, con la conseguente applicazione del medesimo regime giuridico previsto per le attività esternalizzate. Sul tema, v. R. NAYDENOV – D. LIVERI – L. DUPRE – E. CHALVATZI, *op. cit*., 21.

[36] Sul piano nazionale, l'IVASS ha recepito tali indirizzi nell'ambito del Regolamento n. 38/2018 in materia di sistema di governo societario, che disciplina tra l'altro i presidi da adottare nelle esternalizzazioni di funzioni operative essenziali o importanti, imponendo alle imprese obblighi di due diligence preventiva, di

Tuttavia, l'integrazione di servizi *cloud* nel contesto assicurativo comporta anche l'insorgere di nuove vulnerabilità, che si manifestano tanto sul piano tecnico-operativo, quanto su quello giuridico-regolamentare. Il ricorso a fornitori terzi, spesso operanti al di fuori dello Spazio Economico Europeo, solleva questioni in merito alla sovranità, alla localizzazione delle infrastrutture di trattamento dei dati, alla disponibilità, integrità e confidenzialità delle informazioni trattate, nonché alla possibilità per le Autorità di Vigilanza, in particolare IVASS ed EIOPA, di esercitare un controllo effettivo, tempestivo e conforme ai principi di trasparenza e tracciabilità, in linea con quanto previsto dalle citate Linee Guida EIOPA sull'esternalizzazione a fornitori *cloud*[37], dagli obblighi di *audit* previsti dal DORA e dalle garanzie richieste dagli artt. 28 e 44 ss. del GDPR in materia di trasferimento transfrontaliero dei dati.

La crescente dipendenza dal *cloud* comporta, infine, la necessità strutturale, per le imprese assicurative, di rafforzare le competenze interne, attraverso un sistematico aggiornamento delle figure professionali coinvolte nella gestione dei sistemi informativi e nella vigilanza sull'*outsourcing* tecnologico[38]. Si rende imprescindibile, a tal fine, lo sviluppo di politiche aziendali di sicurezza informatica coerenti con gli standard internazionali di riferimento, nonché l'istituzione di strutture di *governance ad hoc*, incaricate di presidiare, in modo continuativo e documentato, i rapporti contrattuali e tecnici con i fornitori di servizi *cloud.*

Le imprese di assicurazione sono, pertanto, tenute a predisporre assetti organizzativi e tecnologici tali da consentire l'integrazione dei servizi *cloud* all'interno della propria architettura informatica in

formalizzazione contrattuale delle responsabilità e di costante verifica sulla qualità e sicurezza dei servizi ricevutiIVASS, Regolamento n. 28 del 3 luglio 2018, *Regolamento recante disposizioni in materia di sistema di governo societario*, in GU n. 168 del 21 luglio 2018, consultabile sul sito istituzionale all'indirizzo https://www.ivass.it/normativa/nazionale/secondaria-ivass/regolamenti/2018/n38/index.html.

[37] EIOPA, *Orientamenti in materia di esternalizzazione a fornitori di servizi cloud*, cit.

[38] Sul ruolo delle autorità finanziarie e della cooperazione nella promozione dei test, v. L. CANNARI, *La resilienza cibernetica del sistema finanziario italiano: il ruolo dei test TIBER-IT*, in *Banca d'Italia – Questioni di economia e finanza (Occasional Papers)*, n. 761, 2023.

condizioni di sicurezza sostanziale e formale. Ciò implica la necessità di garantire, in ogni fase del ciclo di vita del servizio, la completa tracciabilità delle operazioni effettuate, l'adozione di misure tecniche e organizzative adeguate a presidiare la protezione dei dati personali[39] nonché la rigorosa osservanza delle prescrizioni normative applicabili. In tale prospettiva, assumono rilievo centrale le disposizioni contenute nel GDPR, nelle *Guidelines on outsourcing to cloud service providers* di EIOPA, nonché nel d.lgs. 7 settembre 2005, n. 209 (Codice delle Assicurazioni Private – CAP), che impongono agli operatori di assicurare una *governance* solida, trasparente e conforme ai princìpi di *accountability*, minimizzazione del rischio e tutela dell'interesse dell'assicurato.

In particolare, il CAP, che costituisce il *corpus* normativo di riferimento per la disciplina dell'attività assicurativa in ambito nazionale, contempla in maniera puntuale i profili inerenti all'esternalizzazione di funzioni operative rilevanti o critiche. L'art. 30-*ter* sancisce il principio secondo cui l'impresa assicurativa permane integralmente responsabile delle attività affidate a soggetti terzi, ivi inclusi i fornitori di servizi *cloud*, disponendo che l'esternalizzazione non possa in alcun modo pregiudicare la qualità delle prestazioni erogate, la capacità dell'impresa di conformarsi agli obblighi normativi, né tantomeno le garanzie poste a presidio dell'interesse dell'assicurato[40]. In tale prospettiva, è essenziale che i rapporti contrattuali stipulati con i fornitori di servizi *cloud* contemplino specifiche clausole che assicurino la piena trasparenza operativa, l'accessibilità continuativa alle informazioni rilevanti da parte dell'IVASS e la cooperazione con l'autorità di vigilanza, anche in funzione dell'esercizio dei poteri ispettivi e di supervisione prudenziale[41].

[39] Per esempio, i dati idonei a rivelare lo stato di salute, frequentemente trattati nell'ambito del ramo vita e delle coperture sanitarie, che ricadono nella definizione di dati particolari ai sensi dell'art. 9 del Regolamento (UE) 2016/679 e dunque soggetti a specifiche previsioni normative di tutela.

[40] Art. 30-*septies e* 30-*quater* CAP. V anche Reg. IVASS n. 38/2018. Recente è la lettera al mercato in materia di esternalizzazione pubblicata sul sito istituzionale di IVASS in data 12 marzo 2025.

[41] Art. 190-*bis* CAP.

Non può, parimenti, essere trascurata la portata potenzialmente propulsiva che l'adozione del *cloud computing* è suscettibile di esplicare sul piano dell'inclusione assicurativa e dell'estensione dell'accessibilità ai servizi di trasferimento del rischio, in particolare nei confronti di quei segmenti della popolazione collocati ai margini dei tradizionali circuiti distributivi[42]. La possibilità, offerta dalle piattaforme digitali innestate su infrastrutture *cloud* ad elevata disponibilità, flessibilità e resilienza, di strutturare ed erogare prodotti assicurativi in modalità completamente dematerializzata, scalabile e replicabile, consente alle imprese del settore di travalicare i vincoli geografici, infrastrutturali ed economici che storicamente limitano la diffusione della copertura assicurativa.

Tuttavia, l'espansione digitale del mercato assicurativo non può prescindere da un presidio rafforzato dei profili di sicurezza informatica e di tutela del contraente, in quanto esposti a rischi specifici quali il *phishing*, le frodi telematiche, il furto dell'identità digitale e la manipolazione illecita dei dati. Di qui l'esigenza di coniugare l'innovazione nei modelli distributivi con l'implementazione di adeguati strumenti di protezione tecnica e organizzativa, che si traducano nell'adozione di sistemi di autenticazione forte, meccanismi automatici di rilevazione e segnalazione delle anomalie, canali digitali sicuri e accessibili, nonché in una trasparente informazione precontrattuale.

## 3. *Il quadro normativo applicabile alla sicurezza informatica del cloud computing*

### 3.1 *Il quadro emergente dalla normativa orizzontale*

L'evoluzione della normativa europea e internazionale in materia di sicurezza informatica e protezione dei dati ha condotto alla definizione di un articolato quadro giuridico multilivello, all'interno del quale si colloca anche la disciplina relativa al *cloud computing*. Quest'ultima non si esaurisce in una fonte unica, organica e codificata, bensì si

[42] V. NUKALA, *Cloud computing in insurance: emerging trends and transformative technologies*, in *International Journal for ultidisciplinary Research (IJFMR)*, vol. 6, n. 5, settembre-ottobre 2024.

configura come un mosaico normativo in continua evoluzione, composto da regolamenti, direttive di armonizzazione minima, standard tecnici e atti di *soft law*. Tutte queste fonti concorrono alla regolamentazione dei profili di sicurezza, responsabilità, gestione del rischio e continuità operativa nei servizi digitali di nuova generazione.

In tale cornice, uno dei pilastri fondamentali era rappresentato dalla Direttiva (UE) 2016/1148, nota come Direttiva NIS (*Network and Information Systems Directive*), che ha segnato una svolta nell'approccio dell'Unione Europea alla *cybersecurity*, costituendo la prima iniziativa legislativa organica a livello sovranazionale tesa a disciplinare in maniera sistemica la sicurezza delle reti e dei sistemi informativi. Per quanto la normativa sia stata sottoposta a revisione e modifica nel corso di un periodo inferiore ai cinque anni, è utile comprendere il sistema di *governance* e di controlli adottato, per verificare i mutamenti occorsi.

La Direttiva NIS distingueva fra cc.dd. operatori di servizi essenziali e prestatori di servizi digitali, individuando nei primi i soggetti che operavano a livello nazionale nei settori previsti nell'allegato II della Direttiva stessa e offrivano un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali, i cui servizi erano dipendenti dalla rete e dai sistemi informativi; e la cui interruzione a causa di un incidente informativo avrebbe avuto effetti negativi rilevanti sulla fornitura, (cfr. art. 5(1) Direttiva NIS). Invece, i prestatori di servizi digitali si limitavano a tre categorie di fornitori, fra cui in particolare i fornitori di servizi di *cloud computing*.

La normativa europea prevedeva specifici obblighi in materia di gestione del rischio cibernetico, adozione di misure tecniche e organizzative appropriate e notifica tempestiva degli incidenti di sicurezza alle autorità competenti. Nell'ambito del settore assicurativo, i soggetti pubblici e privati ricadevano nella definizione di operatori essenziali e dunque gli obblighi previsti si traducevano nella necessità di rafforzare le misure di protezione dei sistemi *IT* destinati all'erogazione di servizi rilevanti, quali la sottoscrizione, l'emissione e la gestione delle polizze, nonché il trattamento dei dati personali dei contraenti, assicurando al contempo una resilienza adeguata a fronte di attacchi informatici e interruzioni operative.

Spostando l'analisi sui fornitori di servizi *cloud*, tali soggetti erano tenuti a conformarsi con requisiti semplificati e reattivi, giustificate

dalla natura dei loro servizi e delle loro operazioni (consid. 59 Direttiva *NIS*). Per quanto questo approccio stimolasse l'adozione di misure di sicurezza sia da parte degli operatori del settore assicurativo che dei fornitori di servizi *cloud*, nel caso di interazioni fra tali soggetti, la normativa spostava gli oneri di notifica e controllo in capo agli operatori essenziali, in assenza di correlate capacità di controllo e coordinamento.[43]

Questa non era la sola criticità riconducibile all'impianto legislativo. Infatti, altri aspetti sono emersi già nel primo rapporto della Commissione sull'applicazione della direttiva.[44] In particolare, si segnalava (*I*) la frammentarietà dell'attuazione a livello nazionale, con divergenze significative nei meccanismi di vigilanza e sanzione; (*II*) l'assenza di una chiara delimitazione delle categorie soggettive coinvolte, che ha condotto a un'applicazione disomogenea del regime; (*III*) la limitata capacità di affrontare in maniera proattiva minacce transfrontaliere complesse, specie in contesti ad elevata interoperabilità tecnologica come quello assicurativo.

Proprio per superare le carenze ora evidenziate, l'Unione europea ha rivisto la normativa e, nel dicembre 2022, ha adottato la Direttiva (UE) 2022/2555 (cd. NIS *2*), la quale estende in maniera significativa il novero dei soggetti obbligati, introduce un regime sanzionatorio più incisivo e rafforza gli obblighi di *governance* in materia di sicurezza informatica. La NIS 2 individua due categorie di soggetti destinatari: da un lato, le entità essenziali, dall'altro, le entità importanti, entrambe sottoposte a obblighi stringenti di gestione del rischio informatico, notifica obbligatoria degli incidenti di sicurezza, adozione di policy

[43] In particolare, l'Art. 16(5) Direttiva NIS prevedeva in capo all'operatore essenziale l'obbligo di notifica in caso di incidenti che fossero dipesi da una terza parte fornitrice di servizi digitali, richiedendo dunque all'operatore essenziale di svolgere un ruolo di intermediario nei confronti dell'autorità di controllo e/o lo CSIRT nazionale.

[44] COMMISSIONE EUROPEA, *Commission Staff Working Document – Impact Assessment Report – Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*, SWD (2020) 345 final, 16 dicembre 2020.

preventive e reattive, nonché a forme di vigilanza diretta e indiretta parte delle autorità competenti[45].

È da segnalare che nella riforma, la qualificazione dei fornitori di servizi *cloud* è stata modificata parificandone gli obblighi e i requisiti agli operatori del settore assicurativo.[46] Infatti, i fornitori di servizi *cloud* rientrano nel novero delle "entità essenziali". L'Allegato I della direttiva menziona espressamente i tali servizi assoggettandoli a obblighi rafforzati in materia di gestione del rischio, sicurezza delle reti e dei sistemi informativi, e notifica tempestiva degli incidenti di sicurezza.

In tale contesto, il *provider cloud*, qualora fornisca servizi a soggetti operanti in settori critici, come le compagnie di assicurazione e riassicurazione, deve conformarsi a un insieme stringente di requisiti minimi di sicurezza tecnica, *governance* operativa, *business continuity* e capacità di *audit* documentabile. L'inosservanza di tali obblighi può comportare l'irrogazione di sanzioni pecuniarie significative, nonché provvedimenti amministrativi restrittivi, secondo quanto previsto dalla stessa NIS 2, con effetti anche sulla valutazione di idoneità e affidabilità dei fornitori esterni da parte delle imprese assicurative vigilate.

### 3.2 *DORA*

Nel contesto del quadro giuridico multilivello delineato dalle normative europee in materia di *cybersecurity* e protezione dei dati, assume particolare rilievo la disciplina settoriale specificamente

[45] Gli obblighi previsti per le entità essenziali e quelle importanti sono quasi del tutto sovrapponibili, con l'unica differenza in merito agli interventi di vigilanza da parte dell'autorità competente, che nel caso di entità importanti può avvenire solo nel caso in cui vi siano "elementi di prova, indicazioni o informazioni secondo cui un soggetto importante non rispetta presumibilmente la presente direttiva" (Cfr. Art. 34(1) Direttiva NIS 2).

[46] J.D. MICHELS – I. WALDEN, *Cybersecurity, Cloud, and Critical Infrastructure*, in C. MILLARD (a cura di), *Cloud Computing Law*, 2ª ed., Oxford University Press, Oxford, 2021, disponibile su https://academic.oup.com/book/39321/chapter/350586266, ultimo accesso 8 aprile 2026; I. WALDEN – J.D. MICHELS, *Getting Critical: Making Sense of the EU Cybersecurity Framework for Cloud Providers*, arXiv, 9 marzo 2022, disponibile su http://arxiv.org/abs/2203.04887, ultimo accesso 8 aprile 2026.

applicabile al comparto assicurativo[47]. La natura personale dei dati trattati (in particolare nei rami vita e salute), la funzione di pubblica rilevanza svolta dalle imprese di assicurazione e la crescente integrazione di sistemi informatici nell'intero ciclo di vita della polizza, impongono l'adozione di misure rafforzate di sicurezza digitale, supervisionate dalle autorità competenti (*in primis* IVASS ed EIOPA) e declinate secondo i principi di proporzionalità, adeguatezza e responsabilità[48].

La principale innovazione in tale direzione è rappresentata dal Regolamento (UE) 2022/2554, noto come *Digital Operational Resilience Act* (DORA), che si configura come una *lex specialis* in materia di resilienza operativa digitale per il settore finanziario, e dunque anche per le imprese di assicurazione, riassicurazione e distribuzione assicurativa[49]. Il Regolamento si applica, infatti, a una vasta gamma di entità finanziarie, tra cui le compagnie assicurative, imponendo requisiti armonizzati e cogenti in materia di gestione dei rischi *ICT*, segnalazione degli incidenti, test di resilienza operativa, controllo dei fornitori terzi e cooperazione informativa[50].

La relazione tra DORA e NIS 2 è oggetto di peculiare attenzione, giacché entrambe le normative si applicano, in parte, ai medesimi soggetti. Mentre la NIS 2 mira a garantire un livello elevato, uniforme e trasversale di cibersicurezza nei settori essenziali, tra cui è incluso il

[47] Per una lettura del DORA intesa prevalentemente come intervento normativo in materia di cybersicurezza, volto al contenimento dei rischi informatici, si veda anche F. LAUS, *L'amministrazione del rischio. Tra regolazione e procedimento, principio di precauzione e approccio multidimensionale*, Milano, 2023, 450 ss.

[48] Per una prima panoramica v. M. GAGLIARDI – C. D'ELIA, *A Proportional Approach to Cybersecurity Challenges in the Financial Sector: Ideas from Post-Quantum Cryptography Legal Analysis,* in *ITASEC Proceedings,* 2025.

[49] Il Regolamento non ha, ad oggi, suscitato un'attenzione particolarmente diffusa da parte della dottrina; tuttavia, si possono segnalare alcuni contributi di rilievo, tra cui: G. ALFANO, *Rischi informatici nel settore finanziario: strumenti di prevenzione e resilienza operativa digitale*, in *Rivista di Diritto Bancario*, n. 4/2024, 357-397; C.P. BUTTIGIEG – B.B. ZIMMERMANN, *op.cit.*, 11 ss.; D. CLAUSMEIER, *Regulation of the European Parliament and the Council on Digital Operational Resilience for the Financial Sector (DORA)*, in *International Cybersecurity Law Review*, vol. 4/2023, 79 ss.; S. GRIMA – P. MARANO, *Designing a Model for Testing the Effectiveness of a Regulation: The Case of DORA for Insurance Undertakings*, in *Risks*, vol. 9/2021, 206 ss.

[50] Sull'ambito di applicazione, v. art 2 DORA.

comparto assicurativo, il DORA introduce requisiti ulteriori, dettagliati e specifici per il settore finanziario. Il considerando n. 16 del DORA chiarisce che, in caso di sovrapposizione o conflitto tra disposizioni, prevalgono le norme del regolamento, in quanto *lex specialis* rispetto alla normativa orizzontale[51].

Il Regolamento DORA si caratterizza per un approccio integrato, strutturato e prescrittivo, articolandosi in cinque pilastri fondamentali, ciascuno dei quali si traduce in obblighi stringenti che impattano direttamente sull'utilizzo di soluzioni *cloud* da parte delle imprese assicurative. La normativa prevede che il ricorso a fornitori esterni di servizi *ICT*, inclusi i *cloud service provider*, sia ammesso entro i limiti stabiliti dall'art. 3(14), che definisce il concetto di rischio derivante da terze parti *ICT*. L'esternalizzazione di funzioni digitali critiche è pertanto soggetta a un regime di vigilanza indiretta, che impone alle entità finanziarie l'adozione di presìdi organizzativi e contrattuali specifici[52], finalizzati a garantire la continuità operativa, la sicurezza informatica e la cooperazione con le autorità di vigilanza. Fra i requisiti previsti rientrano l'obbligo di condurre una *due diligence* preventiva, la stipula di accordi che prevedano clausole minime obbligatorie, nonché la classificazione del livello di criticità del fornitore e dei servizi affidati[53].

Fra i requisiti previsti, l'art. 28(4)(d) impone agli operatori finanziari di condurre una *due diligence* completa sul potenziale fornitore[54]. Di per sé, si tratta di un requisito ragionevole, ma attraverso questo processo l'istituzione finanziaria deve giungere a una propria

[51] Cfr. considerando 16 DORA.

[52] Cfr. considerando 68 DORA.

[53] La definizione di "*fornitori di servizi ICT terzi*" è ulteriormente chiarita all'art. 3(15) del Regolamento DORA. Secondo questo articolo, si riferisce a un'organizzazione che fornisce servizi digitali e di dati, come servizi di *cloud computing*, *software*, servizi di analisi dei dati e *data center*.

[54] Si veda anche il considerando 73 del Regolamento DORA, il quale chiarisce che i contratti stipulati con fornitori terzi di servizi *ICT* dovrebbero prevedere espressamente clausole che garantiscano all'entità finanziaria, o a soggetti terzi da essa designati, il diritto di accesso, ispezione e *audit* in relazione alle prestazioni fornite, fermo restando l'obbligo di tutela delle informazioni riservate. Tali prerogative risultano essenziali per assicurare un controllo effettivo sull'operato del fornitore e per presidiare in modo continuativo la conformità contrattuale e regolamentare delle attività esternalizzate.

conclusione sull'idoneità o meno di tale fornitore. Questo criterio di idoneità non è definito nel Regolamento DORA e non sono ancora disponibili standard tecnici da parte delle autorità europee di vigilanza.[55] Un'altra valutazione generale che un intermediario finanziario deve effettuare prima di stipulare un contratto con un fornitore di servizi *cloud* riguarda gli standard di sicurezza delle informazioni. Ai sensi dell'art. 28(5), le entità finanziarie possono stipulare accordi contrattuali solo con fornitori terzi di servizi *ICT* che rispettino adeguati standard di sicurezza informatica. Anche in questo caso non è chiaro quali siano tali standard[56].

Un caso specifico è previsto per i cc.dd. fornitori di servizi *cloud* critici (art. 31). Le entità designate come tali sono sottoposti a un regime speciale di vigilanza diretta da parte delle Autorità europee di vigilanza, mediante l'istituzione di un quadro di supervisione *ad hoc*, destinato a presidiare l'affidabilità, la resilienza e la trasparenza dei servizi *ICT* critici, inclusi quelli erogati tramite *cloud*. Tale previsione rappresenta una svolta rispetto all'impostazione tradizionale incentrata sulla sola vigilanza indiretta, e risponde all'esigenza di contenere i rischi sistemici derivanti dalla concentrazione tecnologica. Gli articoli dal 31 al 44 stabiliscono un complesso sistema di controlli[57] che si basa sulla constatazione che un numero ristretto di operatori globali (c.d. *hyperscaler*) fornisce servizi *cloud* a una molteplicità di imprese del settore assicurativo, generando una dipendenza asimmetrica che, in caso di discontinuità operativa o compromissione dei sistemi, potrebbe compromettere la stabilità dell'intero ecosistema assicurativo europeo. Il controllo pubblico su tali operatori diventa, dunque, un imperativo di

[55] Peraltro, tale attività non è prevista fra quelle allocate alle ESAs dall'art. 15 DORA, quindi potrebbe essere dubbia la loro adozione in futuro.

[56] K. PARCHIMOWICZ, *Do Not Get Lost in the Cloud: How EU Financial Institutions Could Avoid Problems with Cloud Services Arising under DORA*, in *Law, Innovation and Technology*, vol. 16/2024, 463, 469.

[57] Numerosi sono i poteri di controllo previsti in capo alle autorità di vigilanza: la valutazione circa la disponibilità di regole, procedure, meccanismi e dispositivi completi, solidi ed efficaci per gestire i rischi *ICT* che può presentare alle entità finanziarie (art. 33(2) DORA), a cui si aggiunge la possibilità di richiedere informazioni e segnalazioni, formulare raccomandazioni (art. 35(1) DORA) e, in caso di inosservanza del regime di segnalazione, il potere di imporre sanzioni (art. 35(6) DORA).

politica normativa e prudenziale, volto a tutelare l'integrità dei mercati, la protezione degli assicurati e la resilienza sistemica.

La scelta da parte degli operatori finanziari verso tali fornitori critici potrebbe avere un impatto ambivalente. Infatti, la vigilanza prevista da parte dell'autorità rappresenterebbe una garanzia di sicurezza ulteriore; d'altra parte, tale scelta contrattuale porterebbe l'operatore finanziario all'interno di una complessa rete di rapporti, in cui potrebbe trovarsi a dipendere da un soggetto legato a numerosi altri enti simili nel sistema finanziario. Non meno rilevante è la possibilità di un impatto indiretto che le decisioni dell'autorità di vigilanza potrebbero avere sullo stesso operatore finanziario[58].

Un profilo che merita autonoma considerazione, e che la letteratura ha sinora sviluppato prevalentemente in relazione al settore bancario, riguarda le implicazioni di *corporate governance* derivanti dal Regolamento DORA. L'art. 5, par. 2, attribuisce all'organo di gestione la responsabilità ultima e complessiva della gestione dei rischi *ICT*, imponendo un coinvolgimento diretto dei vertici aziendali che trascende la dimensione meramente operativa per investire il cuore della funzione di governo dell'impresa. L'organo amministrativo è chiamato a definire, approvare e sorvegliare l'attuazione del quadro di gestione dei rischi *ICT*, a stabilire il livello di tolleranza al rischio informatico e ad assicurare che la strategia digitale dell'impresa sia coerente con la propensione al rischio complessiva. Tali obblighi si traducono, sul piano organizzativo, nella necessità di istituire linee di *reporting* strutturate tra le funzioni *ICT*, le funzioni di controllo interno e l'organo di vertice, nonché nell'obbligo per i membri dell'organo amministrativo di acquisire e mantenere un livello di competenza adeguato in materia di rischi informatici (art. 5, par. 4 ). Il DORA recepisce così, in chiave settoriale, un'evoluzione che la dottrina aveva già delineato in ambito bancario, ove il passaggio da una concezione dei rischi *ICT* come questione esclusivamente tecnica a una loro piena integrazione nella *governance* societaria era stato anticipato dagli *EBA Guidelines on ICT and Security Risk Management* (2019) e dai *BCBS Principles for Operational Resilience* (2021). Come è stato osservato, tale orientamento configura un vero e proprio «dovere di *cyber-literacy*» in capo agli amministratori, la cui violazione può fondare

[58] K. PARCHIMOWICZ, *Do Not Get Lost in the Cloud*, cit. 471.

profili di responsabilità ai sensi dell'art. 2392 c.c., nella misura in cui l'inadeguatezza degli assetti di *governance* del rischio *ICT* si traduca in un pregiudizio per l'impresa o per i soggetti vigilati[59]. Nel contesto assicurativo, questa dimensione assume una rilevanza peculiare, in ragione della funzione sociale dell'attività assicurativa e della centralità dei dati personali, anche di natura sanitaria, trattati nell'esercizio dell'impresa. L'art. 30-*quater* del Codice delle Assicurazioni Private e il Regolamento IVASS n. 38/2018 già imponevano requisiti di adeguatezza organizzativa e di *governance* delle esternalizzazioni; il DORA ne rafforza sensibilmente la portata, elevando la gestione del rischio *ICT* a componente strutturale della *governance* societaria e rendendo gli amministratori direttamente responsabili della resilienza digitale dell'impresa.

Un ulteriore elemento di rilievo è rappresentato, infine, dalle linee guida e dagli orientamenti adottati dalle autorità europee di vigilanza (EBA, EIOPA, ESMA), che nel tempo hanno prodotto numerosi strumenti di *soft law* volti a chiarire le aspettative regolamentari in materia di *governance* della sicurezza *ICT*, gestione dei rischi digitali, risposta agli incidenti e continuità operativa. In particolare, come si è detto, le EIOPA *Guidelines on Information and Communication Technology Security and Governance* rappresentano un riferimento essenziale per le imprese di assicurazione, cui viene richiesto di implementare presìdi organizzativi e tecnici coerenti con il principio di *proportionality* e di *risk-based supervision*, nonché di documentare,

[59] Sul tema della responsabilità degli amministratori per inadeguatezza degli assetti di *governance* del rischio *ICT*, si vedano N. MICHIELI, *Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance*, in *Banca impresa società*, 2024, 252 ss.; G. SCHNEIDER, *IA, rischi d'impresa e le mancate risposte del diritto: … DORA per tutti?*, in N. ABRIANI – R. COSTI (a cura di), *Diritto societario, digitalizzazione e intelligenza artificiale*, Milano, 2023, 145 ss., ove si propone la proiezione del modello DORA sul piano della disciplina generale del diritto d'impresa. Per la letteratura bancaria, cfr. G. SIANI, *La sfida della governance: i nuovi rischi e l'esperienza di vigilanza*, intervento al Convegno ABI "*Supervision, Risks and Profitability 2024*", Milano, 12 giugno 2024; EBA, *Guidelines on ICT and Security Risk Management*, EBA/GL/2019/04, 28 novembre 2019. Per il profilo civilistico della responsabilità gestoria, si veda G. FERRARINI, *Understanding the Role of Corporate Governance in Financial Institutions: A Research Agenda*, in *ECGI Law Working Paper*, n. 347/2017.

monitorare e aggiornare continuamente i propri assetti di sicurezza informatica.

## 4. *Normativa orizzontale sulla sicurezza dei dati personali*

A tale stratificazione normativa si aggiunge, in posizione trasversale e sistemica, il Regolamento (UE) 2016/679, che disciplina il trattamento dei dati personali e impone, a tutti i soggetti coinvolti nella filiera digitale, inclusi i fornitori e gli utenti dei servizi *cloud*, precisi obblighi in materia di sicurezza, *accountability*, minimizzazione e *governance* dei dati. Ai sensi dell'art. 24, il titolare del trattamento è tenuto ad adottare misure tecniche e organizzative adeguate al rischio, mentre l'art. 30 prescrive la tenuta di registri delle attività di trattamento; l'art. 35 richiede, in determinati casi, lo svolgimento di una valutazione d'impatto sulla protezione dei dati (*DPIA*); e gli artt. 33 e 34 disciplinano l'obbligo di notifica all'autorità di controllo e agli interessati in caso di violazione dei dati personali.

Le Linee guida dell'*European Data Protection Board* (*EDPB*), forniscono un'importante chiave interpretativa in ordine alla qualificazione giuridica dei rapporti nei contratti di *cloud computing*, in particolare con riferimento ai concetti di titolare e responsabile del trattamento di cui all'art. 4, punti 7 e 8 GDPR[60]. Secondo tali orientamenti, il *provider cloud* assume normalmente il ruolo di responsabile del trattamento, salvo che determini in autonomia le finalità e i mezzi del trattamento, circostanza che lo qualificherebbe come titolare autonomo, con tutte le conseguenze in termini di obblighi informativi, responsabilità e controlli[61]. La corretta qualificazione giuridica dei ruoli, la stipulazione di clausole contrattuali conformi ai requisiti dell'art. 28 GDPR e l'esercizio di un controllo effettivo sulle modalità di trattamento costituiscono condizioni essenziali per la

[60] V. L. VALLE – B. RUSSO – G. BONZAGNI – D.M. LOCATELLO, *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE*, in *Contratto e impresa/Europa*, n. 1/2018, 343 ss.

[61] W. KUAN HON – C. MILLARD – I. WALDEN, *The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated? – The Cloud of Unknowing*, in *International Data Privacy Law*, vol. 1/2011, 211 ss.; ID., *Who Is Responsible for "Personal Data" in Cloud Computing? – The Cloud of Unknowing, Part 2*, in *International Data Privacy Law*, vol. 2/2012, 3 ss.

conformità del trattamento alle prescrizioni regolamentari e la tutela effettiva dei diritti fondamentali degli assicurati[62].

La più recente giurisprudenza della Corte di Giustizia ha ulteriormente precisato i confini della nozione di *titolare del trattamento,* spostando l'asse interpretativo su un criterio eminentemente funzionale. Con la sentenza del 27 febbraio 2025 (causa C-638/23), la Corte ha infatti chiarito che anche soggetti sprovvisti di personalità giuridica, e dunque privi, secondo il diritto interno, della capacità di essere centro autonomo di imputazione di situazioni giuridiche soggettive, possono nondimeno rivestire la qualifica di titolari del trattamento, ove determinino in concreto le finalità e i mezzi del trattamento dei dati personali[63]. La pronuncia, collocandosi in linea di continuità con l'approccio già fatto proprio dall'EDPB nelle Linee guida del 2020, ribadisce che la qualificazione dei ruoli nel trattamento non può fondarsi su elementi formali o sulla mera auto-attribuzione contenuta in clausole contrattuali, ma deve discendere da un'analisi sostanziale delle funzioni effettivamente esercitate nell'ambito della filiera digitale[64]. In altri termini, la titolarità del trattamento non è un attributo che l'ordinamento conferisce ex lege in ragione della veste giuridica del soggetto, bensì la conseguenza diretta del potere decisionale esercitato in ordine al "*perché*" e al "*come*" dei trattamenti.

Dunque, se è vero che nella prassi l'impresa assicurativa conserva ordinariamente la qualifica di titolare, mentre il *provider cloud* riveste quella di responsabile, è altrettanto vero che tale schema possiede solo

[62] È opportuno segnalare come l'intero impianto normativo europeo sia inserito in un orizzonte dinamico ed evolutivo, in cui il legislatore dell'Unione continua ad aggiornare e integrare la propria strategia digitale. In particolare, il *Digital Services Act* (Regolamento (UE) 2022/2065) e il *Data Governance Act* (Regolamento (UE) 2022/868) introducono nuovi obblighi per i fornitori di servizi digitali e disciplineranno in maniera più organica e sistemica le modalità di accesso, condivisione e riutilizzo dei dati, anche nel contesto assicurativo. È dunque verosimile che il quadro giuridico del *cloud computing*, come applicato alle imprese assicurative, sarà oggetto, nei prossimi anni, di ulteriori interventi normativi, in linea con l'obiettivo strategico di costruire un mercato unico digitale europeo resiliente, sicuro e inclusivo.

[63] CGUE, 27 febbraio 2025, causa C-638/23, *X-FAB Dresden GmbH & Co. KG contro Sächsischer Datenschutzbeauftragter.*

[64] EDPB, *Linee guida 07/2020 sui concetti di titolare e responsabile del trattamento nel GDPR*, adottate il 2 settembre 2020 (versione finale del 7 luglio 2021).

valore presuntivo. Qualora il *provider*, lungi dal limitarsi ad eseguire istruzioni altrui, eserciti una sfera autonoma di determinazione delle finalità o dei mezzi del trattamento – ad esempio sfruttando i dati per proprie analisi di mercato, o scegliendo in maniera indipendente le modalità e i criteri di conservazione – esso non potrà che qualificarsi quale titolare autonomo, con l'assunzione diretta degli obblighi informativi verso gli interessati, delle responsabilità derivanti da eventuali violazioni e dei correlativi poteri di controllo da parte delle autorità di vigilanza.

In questa prospettiva, il principio di *accountability* sancito dall'art. 5, par. 2, GDPR, si rafforza ulteriormente, imponendo al titolare, e in specie alle imprese assicurative, quali soggetti di rilievo sistemico nel mercato finanziario, di dimostrare non soltanto la conformità formale delle proprie scelte contrattuali, ma anche la correttezza sostanziale dell'allocazione dei ruoli e delle responsabilità lungo l'intera catena del trattamento.

L'utilizzo di architetture *IaaS*, *PaaS* o *SaaS*, siano esse pubbliche, private, ibride o *multi-cloud*, non comporta alcuna attenuazione delle responsabilità del titolare, ma anzi ne rafforza la portata, imponendo il rispetto dei principi di liceità, correttezza, trasparenza e sicurezza del trattamento.

Sebbene allo stato attuale non si rinvengano pronunce giurisprudenziali espressamente dedicate alla tematica dell'esternalizzazione del trattamento mediante servizi *cloud*, la giurisprudenza nazionale e sovranazionale ha tuttavia consolidato il principio secondo cui la responsabilità primaria e diretta del titolare del trattamento ai sensi del GDPR permane integra anche qualora il trattamento venga affidato a soggetti terzi, inclusi i fornitori di infrastrutture tecnologiche o di servizi digitali[65]. Tale principio generale

[65] Nella sentenza *UI v. Österreichische Post AG* (causa C-300/21), la Corte di Giustizia dell'Unione Europea ha affermato in modo inequivoco che la responsabilità del titolare del trattamento permane anche in assenza di un danno materiale dimostrabile, qualora il trattamento dei dati personali risulti illecito ovvero privo di idonea base giuridica, richiamando così una concezione oggettiva della responsabilità fondata sull'inosservanza delle prescrizioni del GDPR. Già nella pronuncia *Google Spain* (causa C-131/12), la Corte aveva sancito il principio per cui il soggetto che determina le finalità e i mezzi del trattamento, ai sensi dell'art. 4(7) GDPR, non può sottrarsi agli obblighi giuridici posti in capo al titolare, nemmeno ove affidi integralmente le operazioni materiali a soggetti terzi, come nel caso dei fornitori di

risulta pienamente applicabile, in via estensiva e sistematica, al contesto del *cloud computing*, come altresì evidenziato dall'elaborazione dottrinale e dall'orientamento costante delle autorità garanti, nonché dalle linee guida adottate in sede EDPB[66]. Contrariamente a quanto si

servizi infrastrutturali e digitali. Tale impostazione ha trovato ulteriore conferma nella decisione *Wirtschaftsakademie Schleswig-Holstein* (causa C-210/16), nella quale la Corte ha delineato il profilo della contitolarità del trattamento ai sensi dell'art. 26 GDPR, affermando la possibilità di una responsabilità condivisa anche in assenza di accesso diretto ai dati, laddove più soggetti concorrano, in via anche solo strutturale o funzionale, alla determinazione delle finalità e dei mezzi del trattamento. Un orientamento coerente si rinviene altresì nella giurisprudenza della Corte europea dei diritti dell'uomo, che, nella sentenza *Barbulescu v. Romania* (Grande Camera, ric. n. 61496/08), ha chiarito come la titolarità sostanziale del trattamento, e la conseguente responsabilità, siano da ricondursi alla sfera decisionale del soggetto che determina l'ingerenza nella vita privata dell'interessato, indipendentemente dal fatto che gli strumenti tecnologici impiegati siano forniti o gestiti da soggetti terzi. In questo quadro, l'art. 28 GDPR assume particolare rilievo nei rapporti tra titolare e responsabile del trattamento, imponendo che quest'ultimo fornisca «garanzie sufficienti» per mettere in atto «misure tecniche e organizzative adeguate» affinché il trattamento soddisfi i requisiti del Regolamento e tuteli i diritti dell'interessato. L'utilizzo di soluzioni *cloud* (siano esse *IaaS*, *PaaS* o *SaaS*, in ambienti pubblici, privati o ibridi) configura quindi un'ipotesi di designazione formale di un responsabile del trattamento, che tuttavia non esime il titolare dall'obbligo di controllo e verifica sull'operato del fornitore, né dalla responsabilità sostanziale derivante da eventuali violazioni (cfr. anche art. 5, par. 2, principio di *accountability*). Sul tema, v. D. KAMARINOU – C. MILLARD – F. TURTON, *Responsibilities of Controllers and Processors of Personal Data in Clouds*, in C. MILLARD (a cura di), *Cloud Computing Law*, 2ª ed., Oxford University Press, Oxford, 2021, cap. 9; C. FISCHER ET AL., *Rethinking the Allocation of Roles under the GDPR in the Context of Cloud Computing*, in *International Data Privacy Law*, vol. 14, n. 1/2023, 53 ss.

[66] Specificamente ci si riferisce alle Linee guida 07/2020 elaborate dal Comitato Europeo per la Protezione dei Dati (EDPB) sul concetto di titolare e responsabile del trattamento nelle quali si è espressamente ribadito che il ricorso a fornitori di servizi *cloud* non determina, in alcun caso, un trasferimento di responsabilità in capo a tali soggetti. Al contrario, esso implica la necessità per il titolare del trattamento di instaurare un rapporto giuridico formalizzato, fondato su un contratto conforme ai requisiti dell'art. 28 GDPR, nonché l'obbligo di esercitare una costante attività di supervisione e controllo sull'operato del responsabile, anche mediante *audit*, verifiche documentali e clausole di recesso per inadempimento. Analoga prospettiva è stata delineata dal Garante italiano per la protezione dei dati personali, il quale – con Provvedimento n. 36 del 27 giugno 2013 recante linee guida in materia di *cloud computing* nel settore pubblico – ha sottolineato l'obbligo, in capo al titolare, di procedere a una valutazione preliminare e accurata delle caratteristiche del servizio *cloud* prescelto. Tale valutazione deve estendersi tanto agli aspetti relativi alla

potrebbe ritenere, l'adozione di soluzioni *cloud* non attenua gli obblighi gravanti sul titolare, bensì ne accentua la portata, richiedendo la predisposizione di misure giuridiche e tecniche di particolare rigore, finalizzate ad assicurare la piena conformità del trattamento ai princìpi di liceità, correttezza e trasparenza, come previsto dall'art. 5, par. 1, GDPR, e in un'ottica di effettiva tutela dei diritti fondamentali degli interessati, anche alla luce dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea[67].

In tale prospettiva, si rende imprescindibile la stipulazione di una designazione del responsabile del trattamento conforme ai requisiti di cui all'art. 28 GDPR, recante clausole puntuali in ordine agli obblighi di sicurezza dei dati, ai limiti alla sub-fornitura, ai poteri di *audit* e di verifica riconosciuti al titolare, alle modalità di esercizio dei diritti degli

localizzazione geografica dei dati (con particolare attenzione al rischio di trasferimenti verso Paesi terzi non adeguati), quanto alle misure di sicurezza tecnica e organizzativa offerte dal fornitore, nonché alla sua capacità di garantire la piena conformità alla disciplina europea in materia di protezione dei dati personali. In argomento, vedasi D.P. SINGH, *Securing Privacy in Cloud Computing: A Technical and Regulatory Perspective*, in *Computer Security Journal*, 2023; I. WALDEN – J.D. MICHELS, *Getting Critical: Making Sense of the EU Cybersecurity Framework for Cloud Providers*, in *IEEE Journal on Information Policy*, vol. 10/2022, 23-41.

[67] J. ABRERA, *Data Privacy and Security in Cloud Computing: A Comprehensive Review*, in *Journal of Computer Science and Information Technology*, 2023. Sul punto si vedano: CGUE, sentenza 16 luglio 2020, causa C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems* (cd. *Schrems II*), ove la Corte ha affermato che il titolare del trattamento non può ritenersi esonerato da responsabilità per il solo fatto di aver delegato attività a un responsabile esterno, imponendogli un obbligo attivo di verifica dell'adeguatezza delle garanzie offerte dal fornitore, soprattutto nei casi di trasferimento verso Paesi terzi; Decisione (UE) 2021/914 della Commissione europea del 4 giugno 2021, con la quale sono state adottate le nuove clausole contrattuali standard (SCC) ai sensi dell'art. 46(2) lett. *c*), GDPR, le quali prevedono obblighi rafforzati in termini di sicurezza, *audit*, trasparenza e rimedi contrattuali, divenendo strumento fondamentale per garantire la legittimità dei trattamenti in ambito *cloud* con fornitori extra-UE; nonché *Opinione 5/2012 del Gruppo di lavoro ex art. 29* (*WP29*), che, in un contesto normativo antecedente all'entrata in vigore del Regolamento (UE) 2016/679, aveva già delineato con chiarezza i profili di rischio connessi all'adozione di modelli *cloud*, sottolineando l'esigenza, in capo al titolare, di effettuare un'approfondita attività di *due diligence* nei confronti del fornitore e di disciplinare contrattualmente, con puntuale dettaglio, tutti gli aspetti rilevanti, dalla sicurezza all'eventuale ricorso a sub-responsabili.

interessati[68]. Ove il trattamento comporti il trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali, il contratto dovrà altresì contemplare misure idonee a garantire il rispetto delle disposizioni di cui agli artt. 44 e ss. GDPR, prevedendo l'adozione di strumenti giuridici riconosciuti dall'ordinamento unionale, quali le clausole contrattuali standard o le norme vincolanti d'impresa (*binding corporate rules*) debitamente approvate dall'autorità di controllo competente.

[68] Sul tema si veda EUROPEAN DATA PROTECTION BOARD, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 7 luglio 2021, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en (consultato il 5 giugno 2025), recanti chiarimenti sui concetti di *titolare* e *responsabile del trattamento* alla luce degli artt. 4, nn. 7 e 8, e 28 del GDPR. Tali linee guida, nella loro versione consolidata del 7 luglio 2021, costituiscono uno strumento essenziale per l'interpretazione sistematica delle situazioni in cui più soggetti, in particolare, fornitori di servizi *cloud*, intervengono nella filiera del trattamento dei dati personali. In esse, l'EDPB ribadisce che la qualificazione di un soggetto come *responsabile del trattamento* presuppone che esso agisca per conto del titolare, sulla base di istruzioni documentate, e che non determini in modo autonomo le finalità o i mezzi essenziali del trattamento. Laddove invece il fornitore, anche se formalmente esterno, eserciti un margine decisionale significativo in relazione agli scopi o alle modalità del trattamento, esso dovrà essere qualificato come *titolare autonomo* o, in ipotesi residuali, *contitolare*. In tale prospettiva, i fornitori di servizi *cloud* assumeranno, di regola, il ruolo di responsabili del trattamento, fermo restando l'onere in capo al titolare di valutare *ex ante* la compatibilità di tale inquadramento con la realtà sostanziale del rapporto e di garantire la stipulazione di un contratto conforme all'art. 28(3) GDPR. A completamento di tale inquadramento, in particolare in relazione ai trasferimenti internazionali di dati connessi all'adozione di soluzioni *cloud* fornite da soggetti stabiliti in Paesi terzi, si veda anche EUROPEAN DATA PROTECTION BOARD, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, Version 2.0, 18 June 2021, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en (consultato il 5 giugno 2025). Tali raccomandazioni si pongono nel solco tracciato dalla nota sentenza *Schrems II* (CGUE, C-311/18), che, invalidando il *Privacy Shield* e ridefinendo i parametri per la liceità dei trasferimenti extra-UE, impone ai titolari un dovere proattivo di valutazione della normativa del Paese terzo e della sua compatibilità con i diritti fondamentali degli interessati europei. L'*EDPB*, in particolare, individua una metodologia strutturata in sei fasi, che comprende l'analisi dei flussi di dati, la scelta dello strumento giuridico di trasferimento (quali le clausole contrattuali standard), la valutazione del contesto normativo estero e, se del caso, l'adozione di misure supplementari di natura tecnica, contrattuale o organizzativa.

La liceità del trattamento, nei casi in cui siano coinvolti fornitori stabiliti al di fuori dello Spazio Economico Europeo o si preveda una localizzazione extra-SEE delle infrastrutture, è subordinata alla verifica dell'adeguatezza delle garanzie offerte dal fornitore, alla previa adozione di strumenti giuridici riconosciuti dalla Commissione europea, quali le Clausole Contrattuali Standard (*Standard Contractual Clauses – SCCs*), nonché, ove possibile, alla localizzazione dei dati in ambiti territoriali soggetti a standard normativi equivalenti a quelli europei. Tali accorgimenti rappresentano, pertanto, condizioni essenziali per la legittimità del trattamento e per l'adempimento del principio di *accountability* che permea l'intero impianto del GDPR.

Nel quadro dei requisiti previsti dal GDPR assume particolare rilievo l'art. 32 (1) in cui si alloca sul titolare del trattamento un obbligo di adottare le misure tecniche e organizzative che devono essere proporzionate al rischio e aggiornate in funzione dell'evoluzione tecnologica e della specificità dei trattamenti effettuati.

La lettera della norma riconosce che le migliori prassi tecniche disponibili al momento dell'adozione delle misure di sicurezza assumono rilievo quale parametro interpretativo del principio dello *state of the art*. Dunque, pur non rivestendo carattere cogente, l'adesione volontaria agli standard tecnici internazionalmente riconosciuti in materia di sicurezza informatica si configura quale indice qualificato di diligenza professionale, nonché espressione concreta dell'adempimento degli obblighi di protezione dei dati gravanti sul titolare e sul responsabile del trattamento.

La conformità a tali riferimenti, ancorché non obbligatoria in senso stretto, è valorizzata anche dalla normativa settoriale, con particolare riguardo ai settori finanziario e assicurativo, quale criterio di valutazione della ragionevolezza e adeguatezza delle scelte organizzative e tecnologiche adottate dagli operatori, rilevante tanto ai fini della responsabilità civile, quanto in sede di vigilanza da parte delle autorità competenti.

## 5. *Soft law e standardizzazione*

In tale cornice multilivello, risulta imprescindibile considerare altresì il contributo offerto dagli standard tecnici internazionali che, come anticipato sopra, assumono una funzione sussidiaria e integrativa

nell'interpretazione e nell'attuazione degli obblighi legali in materia di *cybersecurity*, gestione del rischio operativo e protezione dei dati personali[69]. Tali standard, frutto dell'elaborazione congiunta di organismi di normazione riconosciuti a livello globale, forniscono criteri metodologici e presìdi operativi idonei a colmare le lacune della regolazione positiva e a rafforzare il livello complessivo di resilienza organizzativa, in particolare nel contesto della trasformazione digitale e dell'esternalizzazione tecnologica[70].

In parallelo alla normativa dell'Unione, e spesso in funzione complementare ai requisiti da essa imposti, si è progressivamente consolidato un *corpus* di standard tecnici di rilevanza globale, elaborati da organismi quali la *International Organization for Standardization* (*ISO*) e il *National Institute of Standards and Technology* (*NIST*). In questo quadro, la norma ISO/IEC 27001 si pone quale architrave per l'implementazione di un sistema di gestione della sicurezza delle informazioni (*Information Security Management System – ISMS*[71]),

[69] Per una riflessione critica ed esaustiva sul ruolo degli standard nel disegno regolatorio digitale dell'Unione europea, con particolare attenzione alla prospettiva del consumatore e alla funzione para-normativa delle specifiche tecniche nei settori ad alta intensità digitale, si veda H.-W. MICKLITZ, *The Role of Standards in Future EU Digital Policy Legislation. A Consumer Perspective*, luglio 2023, disponibile all'indirizzo https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf.

[70] Gli standard, oltre a svolgere una funzione di coordinamento tecnico e regolamentare, contribuiscono in modo rilevante al rafforzamento della competitività sistemica, generando esternalità positive a livello macroeconomico. Essi facilitano infatti la razionalizzazione dei costi di produzione, l'interoperabilità tra tecnologie, e l'adozione di soluzioni innovative, configurandosi come volano per l'efficientamento dei mercati. In tale prospettiva, la standardizzazione assume altresì una valenza strategica sotto il profilo industriale, in quanto incide sull'allocazione degli investimenti privati, orientandoli verso attività ad alta intensità tecnologica e favorendo, in ultima analisi, un'accelerazione nei processi di trasferimento della conoscenza e della ricerca scientifica in applicazioni industrialmente scalabili (cfr. R.N.A. BEKKERS – K. BLIND – H. COENEN – E. IVERSON – K. JACOBS – K. HOSSAIN, *Case Studies on the Interface Between Research and Standardisation, and Case Studies on Patent Pools as a Coordination Mechanism*, INTEREST Consortium, 2006).

[71] Per sistema di gestione della sicurezza delle informazioni (*ISMS*) deve intendersi quell'apparato organizzativo e procedurale, ispirato a criteri di sistematicità, proporzionalità e miglioramento continuo, volto a presidiare i profili di riservatezza, integrità e disponibilità dei dati trattati da un'organizzazione.

delineando requisiti strutturati per l'analisi, il trattamento e il monitoraggio dei rischi informatici, con implicazioni dirette sulla responsabilità delle imprese assicurative nella protezione dei dati degli assicurati e nella garanzia della disponibilità e dell'integrità dei sistemi informatici. Accanto ad essa, la ISO/IEC 22301 assume una funzione complementare, ponendosi quale strumento di riferimento primario a livello globale per l'implementazione di sistemi di gestione della continuità operativa. Essa delinea un quadro sistematico di requisiti volti a disciplinare la progettazione, attuazione, monitoraggio, riesame e miglioramento continuo di un assetto organizzativo strutturato e documentato, finalizzato ad assicurare la resilienza funzionale dell'impresa e la tempestiva reattività a scenari di discontinuità operativa, quali incidenti informatici, guasti infrastrutturali, eventi naturali o interruzioni nella catena di fornitura digitale[72]. In aderenza a tale impostazione, assumono rilievo integrativo gli standard ISO/IEC 27017 e ISO/IEC 27018, che si pongono in linea di continuità con l'impianto di ISO/IEC 27001, arricchendone il contenuto con prescrizioni specialistiche applicabili all'ambiente *cloud*. In particolare, la ISO/IEC 27017 fornisce linee guida e controlli supplementari rivolti sia ai *provider* sia agli utilizzatori di servizi *cloud*, concernenti la

L'implementazione dell'*ISMS* implica l'adozione di politiche formalizzate, controlli tecnici e organizzativi, procedure di gestione del rischio informatico e misure di monitoraggio e *audit*, secondo un impianto conforme, ove applicabile, ai requisiti internazionali sanciti dalla norma ISO/IEC 27001. Tale sistema, ove correttamente declinato, si configura quale presidio strategico non solo di *compliance* normativa, ma anche di *accountability*, specie nei contesti ad alta intensità regolatoria, quali il settore assicurativo.

[72] Al riguardo pare interessante il confronto con l'art. 2086 c.c., che impone a ogni impresa l'adozione di un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'attività, anche in funzione della rilevazione tempestiva degli indizi di crisi e della perdita della continuità aziendale. I rischi *ICT* possono, infatti, costituire veri e propri *driver* di crisi, con rilevanti implicazioni in termini di sostenibilità operativa e responsabilità dell'organo gestorio. Per un approfondimento, si rinvia a G. SCHNEIDER, *IA, rischi d'impresa e le mancate risposte del diritto: … DORA per tutti?*, in N. ABRIANI – R. COSTI (a cura di), *Diritto societario, digitalizzazione e intelligenza artificiale*, Milano, 2023, 145, ove si osserva come il modello delineato dal DORA risulti «*degno di essere proiettato sul piano della disciplina generale di diritto d'impresa*», in quanto espressivo di un approccio sistemico e preventivo alla gestione del rischio, suscettibile di applicazione anche al di fuori dell'ambito strettamente finanziario.

gestione sicura delle infrastrutture virtualizzate, la segregazione logica dei dati, la configurazione delle interfacce e il controllo degli accessi privilegiati. ISO/IEC 27018, invece, è espressamente orientata alla tutela delle informazioni personali identificabili (*Personally Identifiable Information – PII*) nei contesti di *cloud* pubblico, e promuove l'adozione di principi sostanziali coerenti con il dettato normativo europeo in materia di protezione dei dati personali, tra cui il principio di minimizzazione, la limitazione delle finalità, la trasparenza e l'*accountability* del fornitore.[73]

Il NIST, dal canto suo, ha sviluppato una serie di *framework* e linee guida finalizzati a fornire strumenti operativi per l'identificazione, la protezione, il rilevamento, la risposta e il recupero da eventi di natura cibernetica, secondo un approccio modulare, adattivo e integrabile con le normative vigenti. Il più rilevante ai fini dell'analisi è il *Cybersecurity Framework*, adottato nel febbraio 2014, che individua le misure necessarie per la gestione e riduzione dei rischi per la sicurezza informatica[74]. Il *Framework* è stato poi oggetto di aggiornamento sostanziale nel 2023, ai fini di una migliore applicazione per le piccole e medie imprese che lo utilizzano, nonché per adattarsi alla natura in continua evoluzione della sicurezza informatica[75].

Ulteriori riferimenti significativi sono rappresentati dalle raccomandazioni formulate dall'EIOPA, nonché dalle linee guida del Comitato di Basilea per la vigilanza bancaria (*Basel Committee on Banking Supervision*), le quali, sebbene maturate nell'ambito bancario, enucleano principi fondamentali in materia di resilienza cibernetica, gestione del rischio nella catena di fornitura digitale (*ICT third-party risk management*) e continuità operativa, suscettibili di estensione

[73] P. DE HERT – V. PAPAKONSTANTINOU – I. KAMARA, *The Cloud Computing Standard ISO/IEC 27018 through the Lens of the EU Legislation on Data Protection*, in *Computer Law & Security Review*, vol. 32/2016, 16 ss.

[74] La versione 1.0 del *Framework for Improving Critical Infrastructure Cybersecurity*, sviluppato dal NIST, è stata pubblicata nel 2014, con un focus primario sugli operatori di infrastrutture critiche. Successivamente, nel 2018, è stata introdotta la versione 1.1, che ha mantenuto la piena compatibilità con l'impianto originario, arricchendolo con linee guida aggiuntive su aspetti emergenti, tra cui la gestione del rischio nella *supply chain*. Il testo integrale del *Framework* 1.1 è disponibile al seguente indirizzo: https://www.nist.gov/cyberframework/csf-11-archive.

[75] Si veda il testo finale del *Framework* 2.0 all'inidirizzo https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final.

anche agli operatori del settore assicurativo, in considerazione della crescente convergenza regolatoria e tecnologica tra i due comparti. In particolare, si richiamano le *Guidelines on outsourcing to cloud service providers*[76], che, come si è visto, delineano requisiti sostanziali in ordine alla due diligence preventiva, alla struttura contrattuale, alla gestione del rischio di concentrazione e ai diritti di *audit*. Analogamente, il documento "*Principles for operational resilience*" pubblicato dal BCBS offre un impianto metodologico che, pur riferito agli enti creditizi, si rivela applicabile *mutatis mutandis* anche alle imprese di assicurazione, nell'ottica della prevenzione di discontinuità sistemiche legate a eventi *ICT*[77].

La coesistenza di molteplici standard a livello internazionale ha spinto la Commissione europea a individuare il *cloud computing* come potenziale oggetto di uno schema di certificazione europeo [78]. In questo senso, l'ENISA (*European Union Agency for Cybersecurity*) ha avviato il processo di elaborazione del *Cloud Cybersecurity Certification Scheme*, secondo la procedura prevista dal *Cybersecurity Act*. Tale schema mira a istituire un quadro comune di certificazione per i servizi *cloud*, articolato in tre livelli di garanzia (base, sostanziale, alto), al fine di consolidare la fiducia degli utenti nei servizi certificati, agevolare la valutazione *ex ante* della conformità tecnica e giuridica dei fornitori e semplificare le procedure di due diligence da parte delle imprese assicurative che intendano esternalizzare servizi *ICT* critici. Tuttavia, per quanto lo schema in versione preliminare sia stata oggetto di consultazione nel 2020[79], lo schema non è stato ancora adottato formalmente dalla Commissione Europea.

[76] EIOPA, *Guidelines on outsourcing to cloud service providers*, cit.

[77] BASEL COMMITTEE ON BANKING SUPERVISION, *Principles for operational Resilience*, cit.

[78] È da osservare che già dal 2013, l'ENISA aveva supportato il lavoro della Commissione Europea e la Strategia europea per il *cloud computing* valutando, attraverso incontri con gli *stakeholders* il ruolo degli schemi di certificazione (volontari) nel mercato europeo.

[79] COMMISSIONE EUROPEA, *EU Cloud Certification Scheme*, 9 giugno 2021, disponibile all'indirizzo https://ec.europa.eu/newsroom/cipr/items/713799/en.

## 6. *L'applicazione del sistema multilivello ai diversi tipi di cloud computing: discussione*

L'affidamento a soggetti terzi dell'erogazione di servizi *ICT* mediante architetture *cloud*, siano esse pubbliche, private, ibride o *multi-provider*, configura, a tutti gli effetti, una fattispecie di esternalizzazione tecnologica rilevante ai fini giuridici, che attiva una pluralità di obblighi normativi in capo all'impresa assicurativa. Come delineato sopra, l'Unione Europea, attraverso un insieme stratificato di fonti, ha delineato un sistema di responsabilità multilivello che si articola principalmente su tre assi normativi: la Direttiva NIS 2, il Regolamento DORA e il Regolamento GDPR.

La direttiva NIS 2 ha, come noto, profondamente ridefinito il perimetro soggettivo e oggettivo della disciplina europea in materia di sicurezza delle reti e dei sistemi informativi, ampliando in modo significativo l'ambito applicativo rispetto alla normativa previgente. In tale contesto, le imprese assicurative di dimensioni medio-grandi sono espressamente qualificate come soggetti essenziali, con la conseguenza che sono sottoposte a un regime di *compliance* rafforzato, strutturato su un modello di gestione del rischio ispirato ai principi di prevenzione, reazione e resilienza.

L'art. 21 della direttiva impone a tali entità l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate alla natura, all'entità e alla gravità dei rischi informatici cui sono esposte. Tali misure devono essere formalizzate nell'ambito della *governance* aziendale della sicurezza informatica, documentate a fini di *audit* e riesaminate periodicamente, a testimonianza di un approccio strutturato e dinamico alla gestione della *cyber-resilienza*. Una delle innovazioni più rilevanti introdotte dalla direttiva riguarda l'obbligo di sorveglianza attiva sulla sicurezza dell'intera *supply chain* digitale, con particolare attenzione ai fornitori di servizi *ICT*, inclusi i *cloud service providers*. Le imprese assicurative devono, dunque, considerare i rischi derivanti dalla dipendenza da soggetti terzi, anche in assenza di controllo diretto sulle infrastrutture utilizzate, integrando tali rischi nel proprio sistema di gestione della sicurezza.

Tale approccio trova un riscontro e rafforzamento normativo nel Regolamento DORA, che introduce obblighi stringenti e articolati in materia di gestione delle relazioni contrattuali con i fornitori terzi di

servizi digitali, nel quadro di un disegno regolatorio volto a garantire un controllo effettivo sull'intera filiera tecnologica, a prescindere dal modello tecnico-architetturale adottato.

Sebbene il *cloud* rappresenti uno degli ambiti più critici, il Regolamento si applica all'intera gamma dei servizi *ICT* rilevanti per la resilienza operativa, inclusi *outsourcing* infrastrutturale, sistemi di sicurezza, funzioni di rete, gestione dati e supporto applicativo, indipendentemente dalla modalità di erogazione.

Il DORA impone l'istituzione di un registro interno dei contratti *ICT* (art. 28), la valutazione della criticità dei servizi esternalizzati e l'inclusione nei contratti di clausole minime obbligatorie (art. 30), tra cui si annoverano il diritto di *audit*, l'accesso ai dati e ai sistemi, piani di uscita e continuità operativa, nonché obblighi di cooperazione con le autorità di vigilanza. Come già segnalato, in presenza di fornitori critici si attiva inoltre un regime di vigilanza diretta da parte delle autorità di vigilanza, che segna un passaggio di rilievo dal tradizionale modello di vigilanza indiretta a un sistema di controllo multilivello, volto a presidiare il rischio sistemico derivante dalla concentrazione del mercato *cloud*[80].

Nel contesto delineato dalla NIS 2 e dal Regolamento DORA, il ruolo dei fornitori di servizi *cloud* assume, di conseguenza, una valenza strutturale e non più meramente accessoria, configurandosi come componente critica dell'architettura di sicurezza digitale dell'impresa assicurativa, in quanto nodo strategico della catena del valore informatico e vettore potenziale di rischio sistemico. I *provider* stessi, in funzione della loro rilevanza, possono essere qualificati come entità essenziali o importanti, con conseguente specularità degli obblighi in materia di sicurezza, *governance* e notificazione, in una prospettiva di interoperabilità e di allineamento sostanziale delle politiche di gestione del rischio *ICT*. Un simile allineamento si traduce, tra l'altro, in

[80] Cfr. C.P. BUTTIGIEG – B.B. ZIMMERMANN, *The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision*, cit., 11 ss.; A. SCIARRONE ALIBRANDI, *Innovazione tecnologica, regolazione e supervisione dei mercati*, in V. FALCE (a curadi), *Financial Innovation tra disintermediazione e mercato*, Torino, 2021, 5 ss.; G. SIANI, *La sfida della governance: i nuovi rischi e l'esperienza di vigilanza*, intervento al Convegno ABI "*Supervision, Risks and Profitability 2024*", Milano, 12 giugno 2024, in qualità di Capo del Dipartimento Vigilanza bancaria e finanziaria della Banca d'Italia.

un'esigenza di integrazione concreta dei presìdi di continuità operativa tra assicuratore e *provider*, anche alla luce dei poteri ispettivi e sanzionatori attribuiti alle autorità nazionali di *cybersicurezza*. L'effettività dell'applicazione della normativa varia a seconda del modello di *cloud deployment* adottato. Nei servizi *cloud* pubblici *multi-tenant*, ad esempio, l'impresa assicurativa non dispone di un controllo diretto sulle infrastrutture sottostanti: ciò rende necessario rafforzare i presìdi di auditabilità, tracciabilità, segregazione logica dei dati e clausole contrattuali che garantiscano la reversibilità e la resilienza dell'erogazione del servizio[81]. Al contrario, le soluzioni private o ibride offrono margini di controllo più ampi, ma richiedono comunque un adeguato sistema di *governance* integrata, capace di coprire sia il perimetro interno sia quello affidato a terzi.

A completamento del sistema multilivello delineato dal legislatore europeo in materia di *cybersicurezza*, si innesta la disciplina del GDPR, che impone alle imprese assicurative, nella loro qualità di titolari del trattamento, un complesso di obblighi stringenti volti a garantire la conformità del trattamento dei dati personali ai principi di liceità, correttezza, trasparenza e *accountability*[82].

[81] Nella prassi operativa, molte imprese assicurative incontrano difficoltà nell'ottenere dai fornitori *cloud* clausole contrattuali pienamente conformi agli standard regolatori, specie per quanto riguarda il diritto di *audit*, la localizzazione dei dati e i piani di uscita. Alcuni *provider*, in particolare operatori extra-UE, tendono a imporre modelli contrattuali standardizzati, con limitati margini di negoziazione. A fronte di tali criticità, si stanno diffondendo buone prassi come la creazione di funzioni centrali di controllo sui fornitori critici o l'adozione di sistemi automatizzati di monitoraggio della compliance *ICT*, integrati nei processi aziendali di gestione del rischio.

[82] Sebbene la prassi e la letteratura prevalente qualifichino le imprese assicurative, nell'ambito dell'affidamento a fornitori di servizi *cloud*, come titolari del trattamento ai sensi dell'art. 4(7) GDPR, non mancano profili problematici connessi alla reale autonomia decisionale esercitata da tali soggetti in relazione alle finalità e modalità del trattamento. In presenza di architetture tecnologiche complesse, fortemente standardizzate e predefinite dal fornitore, può infatti risultare opaco il confine tra titolarità sostanziale e mera adesione contrattuale a condizioni imposte *ex ante*. In tali contesti, si potrebbe configurare una forma di co-determinazione materiale che giustificherebbe, quantomeno in parte, una qualificazione in termini di contitolarità o, nei casi più estremi, una riqualificazione del provider in chiave di titolare autonomo per taluni segmenti del trattamento, con conseguenti ricadute sistemiche in ordine alla ripartizione delle responsabilità e agli obblighi di trasparenza verso gli interessati.

L'affidamento a fornitori terzi di servizi *cloud*, in particolare, configura un'ipotesi tipica di trattamento effettuato per il tramite di un responsabile esterno, con conseguente necessità di stipulare un atto giuridico formalizzato, contrattualmente vincolante, che disciplini in modo analitico le istruzioni impartite, le misure di sicurezza applicate, i flussi autorizzati di dati, nonché i meccanismi di *audit*, controllo e cooperazione tra le parti (art. 28(3) GDPR). In particolare, il vincolo contrattuale con il fornitore deve ispirarsi a una logica di responsabilizzazione sostanziale, tale da imporre al titolare del trattamento un obbligo permanente di vigilanza sull'idoneità tecnica e organizzativa del responsabile, da esercitarsi attraverso *audit* sistematici, verifiche documentate e l'impiego di attestazioni rilasciate secondo standard riconosciuti a livello internazionale, quali, ad esempio, la ISO/IEC 27001, *System and Organization Controls 2*. Laddove tale attività di controllo venga surrogata da mere autodichiarazioni unilaterali del fornitore, essa non può, in alcun modo, ritenersi idonea ad esonerare il titolare da responsabilità, conformemente all'interpretazione consolidata delle autorità europee di protezione dei dati.

Ancora più stringente si rivela poi l'onere di presidio giuridico e tecnico in caso di trasferimenti di dati verso paesi terzi non adeguati ai sensi dell'art. 45 del GDPR. In tali ipotesi, l'impresa assicurativa è tenuta a garantire un livello di protezione sostanzialmente equivalente a quello assicurato nell'ordinamento dell'Unione, mediante l'adozione di meccanismi contrattuali vincolanti (clausole tipo, norme vincolanti d'impresa) e, ove necessario, di misure supplementari di natura tecnica o crittografica. Il principio di sovranità digitale si riflette anche sulla pianificazione architetturale delle soluzioni *cloud*, rendendo imprescindibile una mappatura accurata dei *data center*, dei nodi di replica e delle catene di subfornitura coinvolte[83].

[83] Il principio di sovranità digitale, cui fa riferimento anche il legislatore europeo, si colloca all'interno di un'evoluzione strategica più ampia. Iniziative come *GAIA-X*, il *Cloud Rulebook* e l'*European Alliance for Industrial Data*, *Edge* and *Cloud* mirano a rafforzare l'autonomia strategica dell'Unione Europea nel settore dei servizi *cloud*, promuovendo infrastrutture federate e interoperabili, soggette a standard comuni di trasparenza, sicurezza e conformità normativa. Tali sviluppi offrono anche al settore assicurativo l'opportunità di orientare le proprie scelte architetturali in funzione non solo dell'efficienza tecnica, ma anche della resilienza normativa e geopolitica.

Ulteriore rilievo assume l'obbligo di incorporare la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita (*privacy by design* e *by default*, *ex* art. 25 GDPR[84]), il quale implica che ogni scelta tecnologica e organizzativa debba essere subordinata al preventivo svolgimento di un'analisi d'impatto (*Data Protection Impact Assessment*, art. 35 GDPR), in particolare nei casi in cui l'esternalizzazione *cloud* comporti trattamenti su larga scala, profilazione automatizzata o flussi sistematici di dati sensibili. La valutazione d'impatto così delineata deve considerare non soltanto i potenziali effetti lesivi sui diritti e sulle libertà fondamentali degli interessati, ma altresì, e in misura ancor più rilevante, l'interazione sistemica con gli ulteriori profili di rischio tecnologico normativamente disciplinati dalla direttiva NIS 2 e dal Regolamento DORA. Ciò nell'ottica, ormai imprescindibile, di una convergenza regolatoria fondata sull'integrazione organica tra cybersicurezza, resilienza operativa e protezione dei dati personali.

L'applicazione concreta del sistema multilivello di responsabilità delineato dal legislatore europeo in materia di *cybersicurezza* e protezione dei dati deve essere declinata in funzione del modello architetturale di *cloud computing* adottato e del livello di astrazione tecnologica su cui si articola la fornitura del servizio. In particolare, le differenze tra i modelli *IaaS*, *PaaS* e *SaaS*, nonché le varianti architetturali di tipo pubblico, privato, ibrido o federato, incidono in misura rilevante sulla distribuzione delle responsabilità giuridiche e sulla configurazione degli obblighi di compliance.

Nei modelli *IaaS*, l'impresa assicurativa conserva un ampio margine di controllo sulle componenti applicative e sistemistiche, a fronte di una delega limitata all'infrastruttura sottostante: ciò impone un presidio rafforzato delle misure di sicurezza infrastrutturale e dei piani di

[84] Come osservato da M. VEALE – R. BINNS – J. AUSLOOS, *When Data Protection by Design and Data Subject Rights Clash*, in *International Data Privacy Law Review*, 2018, 2, la modificazione lessicale introdotta dal GDPR in tema di *data protection by design and by default* non ha una valenza meramente ideologica, ma riflette un mutamento sostanziale dell'approccio alla tutela dei dati personali, in quanto orientato a garantire *ex ante* la conformità ai principi regolatori. Per un'analisi più ampia e sistematica, v. anche L.A. BYGRAVE, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, in *Oslo Law Review*, vol. 4, n. 2/2017, 105 ss.

continuità operativa, in conformità agli obblighi previsti dalla direttiva NIS 2 e dal Regolamento DORA. Nei modelli *PaaS* e *SaaS*, viceversa, il livello di delega si estende progressivamente sino a comprendere l'intera piattaforma esecutiva o l'applicativo stesso, con la conseguenza che diviene essenziale garantire l'interoperabilità, la tracciabilità delle operazioni e la disponibilità di meccanismi di *audit* formalizzati, specie in contesti *multi-tenant* e ad alta densità di elaborazione dei dati.

Sotto il profilo giuridico, tali configurazioni incidono direttamente sulla qualificazione dei ruoli soggettivi *ex* GDPR, determinando, di regola, l'inquadramento del *cloud provider* quale responsabile esterno del trattamento, con conseguente obbligo del titolare di assicurare la piena conformità dell'architettura contrattuale alle previsioni di cui all'art. 28(3) del Regolamento. In ogni caso, la selezione del modello di *deployment* e la valutazione della sua idoneità sotto il profilo della resilienza normativa devono essere condotte alla luce di un'analisi integrata del rischio, che tenga conto della criticità funzionale dei servizi, della natura dei dati trattati e della possibilità di esercitare un controllo effettivo, anche solo documentale, sull'intera catena tecnologica ed organizzativa. Ne discende, a ben vedere, l'esigenza ormai ineludibile di adottare un modello di *governance* della sicurezza digitale che sia al tempo stesso integrato, interdisciplinare e dinamico, capace di superare la frammentazione degli approcci settoriali e di favorire un coordinamento strutturale e continuo tra le funzioni aziendali coinvolte: *compliance, information technology*, affari legali, *audit* interno e gestione del rischio.

| | **NIS 2** | **DORA** | **GDPR** |
|---|---|---|---|
| ***Infrastructure as a Service (IaaS)*** | Il fornitore di *IaaS* può rientrare tra le "*essential*" o "*important entities*" ai sensi dell'art. 3, lett. a) e b), NIS 2, se | Ai sensi degli artt. 28-31 DORA, il fornitore *IaaS* rientra tra gli *ICT third-party service* | *Ex* artt. 4(7), 28 e 32 GDPR, l'impresa assicurativa agisce come titolare del trattamento, mentre il fornitore *IaaS* è responsabile del trattamento |

| | | | |
|---|---|---|---|
| | fornisce servizi *ICT* fondamentali. L'impresa assicurativa, come "*essential entity*" se supera le soglie dimensionali (allegato I), è tenuta a integrare il rischio derivante dall'*outsourcing* nei propri obblighi di gestione del rischio (art. 21) e a garantire meccanismi di reporting tempestivo degli incidenti (artt. 23-24). | *providers*. Se identificato come critico (art. 31), è soggetto alla supervisione diretta delle ESAs (EIOPA, EBA, ESMA). L'impresa assicurativa ha l'obbligo di classificare il servizio, registrarlo nel "*Register of Information* " (art. 28) e garantire che il contratto includa clausole specifiche su diritti di *audit*, accesso, portabilità e misure di *business continuity* (art. 30). | limitatamente alla componente infrastrutturale. È obbligatoria la stipula di un *DPA* (*Data Processing Agreement*) conforme all'art. 28(3) e l'adozione di misure tecniche e organizzative adeguate alla sensibilità dei dati. Qualora siano coinvolti subfornitori o trasferimenti extra-UE, si applicano le SCC o altre garanzie *ex* artt. 44-46. |

| | | | |
|---|---|---|---|
| ***Platform as a Service (PaaS)*** | In ambito *PaaS*, la Direttiva NIS 2 impone obblighi indiretti sull'assicuratore qualora il servizio *PaaS* supporti infrastrutture critiche (es. motori di calcolo per la determinazione attuariale). In tal caso, l'assicuratore deve garantire, *ex* art. 18, la valutazione della catena di fornitura *ICT*, includendo verifiche sulla sicurezza del *provider PaaS* e sulle capacità di risposta agli incidenti. | Nel modello *PaaS*, se impiegato per funzioni critiche o importanti, DORA impone obblighi di controllo e monitoraggio rafforzato: valutazione della concentrazione del rischio *ICT* (art. 26), inclusione nelle strategie di *exit* e subentro (art. 28(6)), e stipula di accordi contrattuali che prevedano l'accesso alle informazioni, *testing* e cooperazione con le autorità | Nel *PaaS*, la linea di demarcazione tra "*data controller"* e "*data processor"* può risultare sfumata: se il *provider* influenza le modalità tecniche del trattamento (es. configurazione *database, logging, backup*), si può ravvisare una responsabilità autonoma o congiunta (cfr. art. 26 GDPR e *WP29 Guidelines on Controller/Processor*). Occorre un attento scrutinio contrattuale, supportato da DPIA *ex* art. 35 e clausole sul *sub-processing*. |

| | | | |
|---|---|---|---|
| | | competenti (art. 30(2)). | |
| ***Software as a Service* (*SaaS*)** | I fornitori *SaaS*, quando offrono applicativi utilizzati da enti assicurativi rientranti nella direttiva, possono assumere la qualifica di "*important entities*" (art. 3). L'assicuratore è responsabile dell'adozione di misure per garantire la resilienza della catena *ICT* (art. 21), comprese valutazioni del rischio specifico legato al servizio applicativo e contratti che prevedano obblighi di comunicazion | *SaaS* configura *outsourcing* di funzioni critiche se utilizzato, ad esempio, per la gestione dei sinistri, dei contratti o del portafoglio assicurativo. L'impresa assicurativa, ai sensi dell'art. 28, deve identificare, categorizzare e documentare l'accordo, garantendo requisiti minimi su disponibilità, integrità e riservatezza del servizio. Il *provider* deve cooperare nell'ambito degli scenari di crisi *ICT* e | Il provider *SaaS*, se determina le finalità o i mezzi essenziali del trattamento (es. scelta degli algoritmi di gestione sinistri o di scoring), può assumere il ruolo di titolare o contitolare. È fondamentale garantire i diritti degli interessati *ex* artt. 12-22, in particolare portabilità (art. 20) e diritto alla cancellazione (art. 17), spesso complessi da esercitare su architetture *SaaS* chiuse. Il contratto deve riflettere obblighi di sicurezza *ex* art. 32 e gestione delle violazioni *ex* art. 33. |

| | | | |
|---|---|---|---|
| | e degli incidenti. | garantire continuità operativa, con reportistica periodica sulle *performance* (artt. 28, 30, 32). | |

***Tabella 1*** – Obblighi normativi multilivello per i modelli di *cloud computing* (*IaaS*, *PaaS*, *SaaS*) nel settore assicurativo ai sensi della Direttiva NIS 2, del Regolamento DORA e del GDPR.

| | **NIS 2** | **DORA** | **GDPR** |
|---|---|---|---|
| ***Cloud* pubblico** | Nel *cloud* pubblico, dove l'infrastruttura è condivisa, il *provider* può rientrare tra le "*essential*" o "*important entities*" ai sensi dell'art. 3 NIS 2. Le imprese assicurative che operano in tale contesto devono garantire la protezione dei dati e dei | Nel *cloud* pubblico, i fornitori sono spesso soggetti terzi critici per funzioni assicurative digitali (es. piattaforme di emissione polizze o gestione sinistri *online*). L'art. 28 DORA impone alle imprese assicurative la tenuta del registro delle relazioni contrattuali *ICT* e l'obbligo di | Nel *cloud* pubblico, il trattamento di dati personali da parte delle assicurazioni richiede solide garanzie contrattuali e tecniche *ex* artt. 28 e 32 GDPR. I trattamenti ad alto rischio (es. dati sanitari, biometrici) impongono una *DPIA* (art. 35). Il trasferimento |

| | | | |
|---|---|---|---|
| | sistemi connessi a funzioni critiche (es. sottoscrizione, gestione sinistri), assicurando la conformità agli artt. 21-24 NIS 2 in materia di *governance* e notifica degli incidenti. | implementare piani di uscita e resilienza (art. 30). | verso paesi terzi dev'essere conforme agli artt. 44-46. |
| ***Cloud* privato** | Nel *cloud* privato, se gestito internamente, la responsabilità ricade interamente sull'impresa assicurativa, che deve comunque adempiere agli obblighi dell'art. 21 NIS 2 per la protezione delle reti e dei sistemi. Se il servizio è affidato a terzi, occorre verificare la classificazione dell'*outsourcer* | Nel *cloud* privato, se gestito internamente, l'impresa assicurativa mantiene il controllo diretto. Se esternalizzato, deve applicare pienamente i requisiti di contrattualizzazione *ICT ex* artt. 28-30 DORA, garantendo misure di sicurezza, disponibilità e accesso per le autorità di vigilanza. | Nel *cloud* privato, le assicurazioni godono di maggiore controllo diretto sui trattamenti. Tuttavia, se l'infrastruttura è gestita da terzi (es. *private cloud provider*), resta necessario un *DPA* e la verifica del rispetto degli obblighi di sicurezza, minimizzazione e integrità dei dati (artt. 5, 28, 32). |

| | | | |
|---|---|---|---|
| | e le eventuali ricadute sulla continuità operativa assicurativa. | | |
| ***Cloud* ibrido** | Nel *cloud* ibrido, le imprese assicurative devono garantire l'interoperabilità dei sistemi e la coerenza dei presìdi di sicurezza tra ambienti *cloud* pubblici e privati. Ai sensi degli artt. 18 e 21 NIS 2, devono essere definiti meccanismi integrati di valutazione e risposta ai rischi *cyber* che coinvolgano più soggetti. | Il *cloud* ibrido richiede la tracciabilità e classificazione di ciascun segmento funzionale assicurativo (es. archiviazione contratti, gestione sinistri) secondo gli artt. 25 e 28 DORA. L'impresa deve verificare che i fornitori rispettino i requisiti di *testing*, auditabilità e protezione dei dati operativi. | Nel *cloud* ibrido, i dati relativi a clienti, contratti, sinistri e profili di rischio devono essere trattati con modalità interoperabili e conformi in ogni ambiente. L'impresa assicurativa deve documentare la ripartizione delle responsabilità e garantire la piena esercitabilità dei diritti dell'interessato (artt. 12-22). |
| **Modello *multi-cloud*** | Nel modello *multi-cloud*, le imprese assicurative devono affrontare sfide complesse | Nel *multi-cloud*, le imprese assicurative devono affrontare i rischi di concentrazione e incompatibilità | Il *multi-cloud* espone le imprese assicurative a rischi di sovrapposizione e contrattuale e |

| | | | |
|---|---|---|---|
| | legate alla frammentazion e contrattuale e alla gestione della resilienza operativa. L'art. 18 NIS 2 impone il presidio della catena di fornitura digitale e l'obbligo di garantire l'adeguatezza dei fornitori sotto il profilo della sicurezza informatica. | contrattuale. DORA (art. 26) richiede strategie di diversificazione e *governance* dei fornitori, contratti standardizzati, e l'inclusione di tutti i *provider* nel "*Register of Information*". | incoerenza tra le *policy privacy* dei diversi fornitori. Occorre assicurare un governo unificato dei trattamenti, con responsabilità centralizzata e meccanismi di *audit* estesi (artt. 24 e 28). |

***Tabella 2*** – Obblighi normativi multilivello nei modelli architetturali di *cloud deployment* nel settore assicurativo (*cloud* pubblico, privato, ibrido e *multi-cloud*)

## 7. *L'insufficienza dell'adozione di standard come criterio esclusivo di conformità giuridica*

Il concetto di *compliance*, inteso quale complesso sistemico di attività organizzative, tecniche e documentali finalizzate ad assicurare la conformità dell'agire aziendale all'ordinamento giuridico vigente, si è arricchito, nel contesto digitale, di una dimensione ulteriore e strategica: la gestione della sicurezza informatica attraverso l'adozione di standard tecnici[85]. Nel settore assicurativo, tale evoluzione si è

[85] Come rilevano A. BERTOLINI – R. LIMONGELLI, *Regulatory frameworks and standards for agricultural robotics in the European Union,* in E. VAN HENTEN – Y. EDAN (a cura di), *Advances in agri-food robotics, 2024, 461-479*, gli standard rappresentano strumenti di elevata utilità, volti a codificare le buone pratiche attraverso il contributo congiunto di esperti del settore e della comunità accademica,

tradotta in un progressivo ricorso a *framework* normativi, prassi operative, certificazioni accreditate e standard internazionali, che operano come strumenti sussidiari per garantire la resilienza operativa, la continuità del servizio e la protezione del dato assicurativo, anche in chiave reputazionale e sistemica.

Tuttavia, sorge l'interrogativo se l'adozione di tali standard possa ritenersi di per sé sufficiente a esaurire gli obblighi di conformità giuridica gravanti sulle imprese assicurative. A tale riguardo, occorre sin da subito chiarire che il rispetto degli standard tecnici, pur rappresentando una condizione necessaria ai fini della *due diligence* e della diligenza professionale, non costituisce condizione sufficiente per soddisfare integralmente le prescrizioni normative vincolanti. Il diritto positivo europeo, come si evince con chiarezza dal GDPR, dalla Direttiva NIS 2 e dal Regolamento DORA, esige un approccio sostanziale, in cui l'effettività delle misure adottate prevale sulla loro mera apparenza formale o conformità procedurale.

Nel contesto del GDPR, l'art. 32 stabilisce che il titolare e il responsabile del trattamento debbano adottare "*misure tecniche e organizzative adeguate*" al rischio. Il concetto di adeguatezza implica una valutazione contestuale, dinamica e proporzionata, che tenga conto dello stato dell'arte, dei costi di attuazione, della natura e finalità del trattamento, nonché del rischio per i diritti e le libertà fondamentali delle persone fisiche. Gli standard internazionali, quali la ISO/IEC 27001 o la ISO/IEC 27701, rappresentano strumenti di supporto alla conformità tecnica, ma non esimono l'impresa assicurativa dal dovere di motivare *ex ante* ed *ex post* la scelta, l'implementazione e l'adeguatezza delle misure rispetto al rischio effettivamente affrontato.

Un'analoga impostazione si rinviene nella Direttiva *NIS* 2, la quale, all'art. 21, impone ai soggetti essenziali e importanti, tra cui rientrano, come si è osservato, le imprese assicurative, di adottare misure tecniche, operative e organizzative adeguate e proporzionate alla natura, all'entità e alla gravità dei rischi per la sicurezza dei sistemi informativi e delle reti. Anche in questo caso, il richiamo agli standard

costituendo, di fatto, uno degli output più rilevanti dell'attività di ricerca. In quanto prodotti ben strutturati e riconosciuti, essi concorrono significativamente allo sviluppo della regolazione, sia a livello nazionale che internazionale, e svolgono oggi un ruolo di primaria importanza nei processi di normazione dell'Unione europea e dei suoi Stati membri.

è implicito, fungendo da parametro tecnico di riferimento, ma non può sostituirsi a una valutazione puntuale, casistica e contestualizzata delle specificità aziendali, che spetta alla singola impresa assicurativa svolgere sotto la propria responsabilità.

Il Regolamento DORA, pur riconoscendo il ruolo degli standard tecnici, segnatamente in materia di *testing* di resilienza operativa, gestione degli incidenti *ICT*, e *governance* della sicurezza contrattuale, non adotta un approccio meramente formalistico, ma impone all'impresa assicurativa una responsabilità sostanziale nella definizione, adozione e monitoraggio di un sistema interno di gestione dei rischi digitali, calibrato in relazione alla complessità organizzativa, al livello di esposizione al rischio *ICT*, alla criticità delle funzioni esternalizzate e all'eventuale interconnessione con fornitori terzi di servizi *cloud*.

Ne discende che gli standard tecnici, per quanto autorevoli e diffusamente adottati, devono essere intesi quali strumenti ausiliari di natura metodologica, parametri orientativi di *best practice* e supporti funzionali alla dimostrazione della diligenza professionale, ma non possono in alcun modo considerarsi esaustivi rispetto al complesso degli obblighi prescrittivi derivanti dalla normativa vigente[86]. Tali standard, infatti, agevolano i processi di *audit* interno ed esterno, concorrono alla tracciabilità documentale delle scelte organizzative e tecnologiche, e facilitano l'interlocuzione con le autorità di vigilanza, fungendo da elemento di riferimento nella verifica della compliance.

Ciononostante, essi non esonerano l'impresa assicurativa dall'obbligo di effettuare una valutazione puntuale, dinamica e contestualizzata dell'adeguatezza e dell'efficacia delle misure adottate, da condursi in rapporto al rischio effettivamente presente nel proprio perimetro operativo, alla natura delle attività trattate, nonché alla criticità delle funzioni digitali esternalizzate. In questo senso, la conformità normativa si configura non come mera adesione formale a un repertorio di standard codificati, bensì come esercizio sostanziale di responsabilità organizzativa, sorretto da processi decisionali documentati, verificabili e soggetti a riesame periodico, in linea con i

[86] È interessante l'analisi offerta da C. KOOLEN – K. WUYTS – W. JOOSEN – P. VALCKE, *From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models*, in *Computer Law & Security Review*, 2024.

principi di *accountability*, proporzionalità e *risk-based approach* che informano l'intero impianto regolatorio europeo.

Un ulteriore profilo critico riguarda la distinzione tra standard orizzontali e verticali. I primi, aventi natura generalista, sono destinati ad applicarsi in modo trasversale a una pluralità di settori economici e organizzativi, offrendo un quadro metodologico di riferimento ampio e astratto, come avviene per la ISO/IEC 27001 in materia di sistemi di gestione della sicurezza delle informazioni, la ISO/IEC 22301 sulla continuità operativa, o le ISO/IEC 27017 e 27018, specificamente orientate alla sicurezza e protezione dei dati in ambienti *cloud*. Gli standard verticali, per converso, si caratterizzano per un elevato grado di specializzazione settoriale, essendo concepiti per tenere conto delle peculiarità operative, regolatorie e di rischio tipiche di uno specifico comparto[87].

[87] In ambito assicurativo, esempi sono le *EIOPA Guidelines on ICT Security and Governance* e gli *Implementing and Regulatory Technical Standards* sviluppati nell'ambito del quadro Solvency II, i quali declinano i principi generali in prescrizioni tecniche mirate e conformi alle esigenze di vigilanza del settore.

| **Standard / data ultima revisione o pubblicazione** | **Rilevanza** | **Riferimenti normativi** |
|---|---|---|
| **ISO/IEC 27001** 2022 (3ª edizione)[88] | Standard quadro per *ISMS*, richiesto per strutture *ICT* critiche. Rilevante per la *compliance* con DORA artt. 5 e 15 | *EIOPA Guidelines on ICT Security and Governance* (GL 2019/04) §13-18 |
| **ISO/IEC 27017** 2015 | Riferimento tecnico per le misure di sicurezza specifiche nei contratti *cloud* | *EIOPA Guidelines on Outsourcing to Cloud Providers* (GL 2020/07) §23-31 |
| **ISO/IEC 27018** 2019 (2ª edizione) | Protezione dei dati personali nel *cloud*. Essenziale per fornitori *SaaS/PaaS*. | Art. 28 GDPR + *WP29 Opinion 05/2012 on cloud computing* |
| **ISO/IEC 22301** 2019 (2ª edizione)[89] | Standard per la continuità operativa, utile anche per i piani di uscita previsti da DORA. | DORA artt. 11-13 (*Business Continuity e Disaster Recovery*) |
| **ISO/IEC 27701** 2019[90] | Integra gestione del rischio e *accountability privacy*, utile per *audit* interno. | Estensione privacy della ISO 27001. Allineato a GDPR artt. 24-32 |
| **ISO/IEC 31000** 2018 (2ª edizione) | Quadro di riferimento per l'integrazione del *risk management* tradizionale e *ICT*, utile per l'implementazione coerente con DORA e NIS 2 | Art. 5 DORA; art. 21 NIS 2; applicazione trasversale alla gestione del rischio *ICT* |
| **ISO/IEC 20000-1** 2018 (3ª edizione)[91] | Strutturazione della gestione dei servizi *IT*, utile per il controllo dei fornitori *cloud* e la *compliance* contrattuale assicurativa | Artt. 28-30 DORA (outsourcing *ICT*); *EIOPA GLs on Outsourcing* (2020) |

[88] L'ultimo aggiornamento è del febbraio 2024, con l'*amendment* 1 relativo ai cambiamenti climatici.

| | | |
|---|---|---|
| **ISO/IEC 27036-4** 2016 | Supporto alla valutazione della sicurezza e resilienza della *supply chain ICT*, centrale in ambienti *multi-cloud* e *outsourcing* assicurativo | Art. 18 NIS 2 (*supply chain*); DORA art. 28(6) |
| **ISO/IEC 29184** 2020[92] | Standard specifico per la trasparenza delle informative privacy *online* e la raccolta del consenso in ambienti digitali e *cloud* | Artt. 5, 7, 12-14 GDPR*; EDPB Guidelines* 07/2020; Provv. Garante n. 224/2021 |
| **ISO/IEC 20889** 2018 | Definisce metodi tecnici per l'anonimizzazione e la pseudonimizzazione, rafforzando il principio di minimizzazione del GDPR | Artt. 5(1)(c), 32 GDPR; utile per *accountability* e *data minimization* |
| **ISO/IEC 27560** 2023 | Supporta le imprese assicurative nella conduzione di DPIA articolate e documentate, in coerenza con il principio di *accountability* | Art. 35 GDPR (DPIA); *EDPB Guidelines on DPIA* (WP248 rev.01) |
| **ISO/IEC 27557** 2022 | Definisce requisiti e linee guida per la gestione della privacy differenziata in base al contesto e alla sensibilità | Artt. 5(1)(c), 25, 32 GDPR (minimizzazione, *privacy by design*); EDPB *Guidelines on* |

[89] L'ultimo aggiornamento è del febbraio 2024, con l'*amendment* 1 relativo ai cambiamenti climatici.

[90] Attualmente in fase di revisione.

[91] L'ultimo aggiornamento è del febbraio 2024, con l'*amendment* 1 relativo ai cambiamenti climatici

[92] Standard attualmente in fase di revisione sistematica.

| | | |
|---|---|---|
| | dei dati, utile per imprese assicurative che offrono servizi digitali personalizzati. Promuove l'approccio *risk-based* e la minimizzazione del trattamento | *Data Protection by Design and by Default* (2020) |
| **ISO/IEC 27040** 2024 (2ª edizione) | Linee guida sulla sicurezza dello *storage*, essenziale per sistemi *cloud*, *backup* e archiviazione assicurativa | Art. 32 GDPR; DORA art. 9(2); NIS 2 art. 21 |
| **ISO/IEC 27042** 2015 | Standard forense digitale per analisi degli incidenti, utile ai fini investigativi e documentali in ambito assicurativo | DORA art. 11; DORA Allegato II; NIS 2 art. 23 |
| **ISO/IEC 27050-1** 2019 (2ª edizione) | Guida alla conservazione e analisi di evidenze digitali, rilevante per la documentazione *post-breach* | Artt. 5(2), 33-34 GDPR; DORA art. 17 |
| **ISO/IEC 27002** 2022 (3ª edizione) | Aggiornamento dei controlli ISO 27001, utile per rafforzare la postura di sicurezza delle imprese assicurative | DORA Allegato II; ISO/IEC 27001:2022 complementare |
| **ISO/IEC 27561 (draft)** | Modello strutturato per la gestione documentata del consenso, utile nei portali assicurativi *online* | Art. 7 GDPR; *EDPB Guidelines 05/2020 on consent* |
| **ISO/IEC 23894** 2023 | Riferimento per la gestione dei rischi derivanti da algoritmi *AI*, importante per | *AI Act* + applicazione in ambito *InsurTech* |

| | | |
|---|---|---|
| | applicazioni *InsurTech* e *underwriting* | |
| **ISO/IEC 27001-4 (draft)** | Applicazione tecnica per la protezione di ambienti virtualizzati, *container* e microservizi usati in architetture *cloud* | Applicazione tecnica per ambienti containerizzati – DORA art. 15 |
| **NIST SP 800-53** Rev. 5.1.1 7 novembre 2023[93] | Catalogo completo di controlli tecnici e organizzativi. Utilizzabile per audit interni e terzi. | Riferito nel *Cyber Resilience Oversight Expectations* (EIOPA, 2019) |
| **NIST SP 800-37** Rev. 2 20 dicembre 2018[94] | Fornisce il *framework* metodologico per implementare un ciclo di vita di gestione del rischio *ICT*. | DORA allegato II (gestione del rischio *ICT*) |
| **NIST SP 800-92** Rev. 1 11 ottobre 2023[95] | *Standard* per *log management* e *audit trail*, richiesto per *incident response* e *accountability* GDPR | Art. 30 DORA; art. 33 GDPR |
| **NIST CSF 2.0** 26 Febbraio 2024 | Usato come base per strategie *cyber* e gestione del rischio operativo; utile per valutazioni periodiche | DORA art. 5(2), *EIOPA ICT Guidelines* 2019/04 §19 |
| **ENISA Cloud Security Controls** | Set minimo di controlli tecnici e organizzativi per *cloud provider*; guida per classificazione e | NIS 2 Allegato I; *ENISA Guidelines* 2022 e 2023; supporto alla valutazione dei fornitori |

[93] Data di pubblicazione originale della Revisione 5: 23 settembre 2020.

[94] L'ultimo aggiornamento risale, tuttavia, al 23 aprile 2021.

[95] Bozza in fase di revisione; periodo di commento pubblico chiuso il 29 novembre 2023.

| | | |
|---|---|---|
| 24 maggio 2023 | sorveglianza dei fornitori *ICT* | |
| **COBIT 2019** 14 novembre 2018 | Framework di riferimento per la *governance ICT* e il raccordo tra *risk management*, *audit* interno e *compliance* regolatoria | Art. 15 DORA (*ICT governance*); DORA Allegato II; supporto all'*audit* interno |
| **CSA Cloud Controls Matrix 4.0** 3 giugno 2024 | Matrice di controllo adatta alla *due diligence cloud*, usata per validare la conformità alle normative e agli standard tecnici | Mappatura con ISO 27001, 27017, NIST SP 800-53; utile per *audit cloud compliance ex* DORA |
| **Basel Principles on Operational Resilience** 31 Marzo 2021 | Rilevante per sviluppare strategie di continuità operativa, risposta agli incidenti e resilienza assicurativa secondo DORA | DORA artt. 11-13; considerato nel dialogo intersettoriale tra EIOPA, EBA e ESRB |

***Tabella 3*** – Quadro di riferimento tecnico-normativo per la compliance multilivello nel settore assicurativo.

L'adozione combinata di standard orizzontali e verticali può innalzare in modo significativo il livello di *compliance* sostanziale, a condizione che sia accompagnata da un monitoraggio costante del rischio, da politiche interne formalizzate, da percorsi di formazione continua e da meccanismi efficaci di responsabilizzazione dei vertici aziendali. In tale prospettiva, la certificazione accreditata, come quella prevista dal *Cybersecurity Act*, può costituire una presunzione relativa di conformità tecnica, ma non libera in alcun caso l'impresa dalle responsabilità legali connesse alla lesione di diritti protetti o all'insorgenza di eventi pregiudizievoli prevenibili.

È pertanto opportuno promuovere un approccio multilivello e integrato alla *compliance*, che non si limiti all'adozione di strumenti tecnici, ma comprenda anche politiche aziendali di sicurezza, sistemi di

audit e controllo interno, formazione periodica del personale, aggiornamento normativo continuo e impegno attivo della dirigenza nella cultura della sicurezza e della responsabilità. Il principio di *accountability*, comune a tutte le normative europee di settore, impone infatti non solo di conformarsi alla norma, ma di essere in grado di dimostrare, anche in sede ispettiva o contenziosa, l'efficacia, l'adeguatezza e la proporzionalità delle misure adottate.

## 8. *Riflessioni sistemiche sull'equilibrio tra innovazione digitale e conformità regolatoria nel settore assicurativo*

L'analisi qui condotta mostra come l'adozione del *cloud computing* nel settore assicurativo europeo non si esaurisca in un aggiornamento tecnico, ma segni una trasformazione strutturale dell'ecosistema organizzativo e regolatorio entro cui l'impresa opera; il *cloud*, nelle sue declinazioni architetturali e nei modelli *IaaS-PaaS-SaaS,* diviene l'infrastruttura abilitante dell'impresa digitale, permeando processi, dati e relazioni con gli assicurati. Questa metamorfosi si colloca in un quadro multilivello, nel quale norme orizzontali (GDPR, NIS2) e strumenti settoriali (DORA), insieme a *soft law* e standard tecnici, concorrono a definire obblighi, presìdi e responsabilità senza tuttavia comporsi in un disegno perfettamente lineare: sovrapposizioni e interstizi interpretativi impongono una compliance non meramente dichiarativa ma sostanziale, capace di integrare diritto, tecnologia e gestione del rischio[96].

In tale prospettiva, gli standard internazionali operano come grammatica operativa della conformità: traducono precetti legali in controlli e procedure verificabili, senza però assurgere a *passe-partout* autonomi, giacché la loro efficacia dipende dall'innesto in una governance consapevole delle specificità di mercato, della geografia

[96] Lo rileva anche G. DE DONNO, *op. cit.,* 241, riportando l'intervento del dott. Pietro Ranieri, il quale ha sottolineato l'intensificarsi della produzione regolatoria a livello unionale, con l'introduzione di nuovi strumenti in materia di sostenibilità (quali *SFDR*, Tassonomia, *CSRD*, *CSDDD*), che vanno a sovrapporsi o intrecciarsi con discipline già vigenti o in via di definizione (*Solvency II*, Basilea, *IDD*, *MiFID*), delineando un quadro complesso che rischia, tuttavia, di risultare di difficile intelligibilità per il consumatore finale, il quale si confronta con le imprese vigilate nella prospettiva di perseguire obiettivi di investimento e protezione.

normativa e della filiera tecnologica. Proprio la filiera, stratificata in livelli di fornitura e subfornitura, dove servizi *PaaS* critici insistono su infrastrutture *IaaS* di *hyperscaler* globali, dilata il perimetro del rischio e della responsabilità: la dipendenza asimmetrica e la propagazione degli obblighi di *audit*, certificazione e controllo discendono lungo la catena *ICT*, imponendo *due diligence* rafforzata e visibilità *end-to-end* sugli elementi che sostengono la continuità operativa e la tutela degli assicurati[97].

Ne deriva che la protezione dei dati personali, pur centrale, è un tassello di un mosaico più ampio, che comprende resilienza operativa, stabilità di sistema, trasparenza e fiducia del mercato; e che il *cloud*, lungi dall'essere un'opzione neutra, assume il rilievo di infrastruttura vitale con riflessi di *accountability*, sicurezza pubblica e vigilanza regolatoria. Da ciò discende l'impossibilità di ridurre la conformità a un adempimento statico: essa va concepita come processo continuo, interdisciplinare e adattivo, fondato su politiche interne robuste, competenze aggiornate, tracciabilità decisionale e leale cooperazione con le autorità[98].

Un esempio concreto può illustrare la portata pratica dell'esigenza di *compliance* sostanziale e integrata. Si consideri il caso di un'impresa assicurativa operante nel ramo vita che affidi a un *hyperscaler* statunitense, in modalità *SaaS*, la piattaforma di gestione dei sinistri, comprensiva del trattamento di dati sanitari degli assicurati. Un incidente di sicurezza informatica che determini l'esfiltrazione di tali dati attiva simultaneamente obblighi riconducibili a ciascuno dei tre assi normativi analizzati. Sul versante del GDPR, l'impresa, nella sua qualità di titolare del trattamento, è tenuta a notificare al Garante entro

[97] H.S. SCOTT – J. GULLIVER – H. NADLER, *Cloud Computing in the Financial Sector: A Global Perspective*, cit., 4-5. V. anche W. KUAN HON – C. MILLARD, *Banking in the Cloud: Part 1 – Banks' Use of Cloud Services*, cit., 4-6.

[98] Come evidenzia V. R. DEB CHAKLADAR*, op. cit*., 14, le tecnologie *cloud* pongono la protezione dei dati quale priorità strategica, gestendo infrastrutture globali secondo standard di sicurezza e *compliance* particolarmente rigorosi. Ciò permette alle imprese assicurative di adempiere agli obblighi normativi in materia di trattamento dei dati, garantendo al contempo la tutela delle informazioni sensibili della clientela. I fornitori di servizi *cloud* investono in modo significativo in misure di sicurezza avanzate, quali la crittografia dei dati, l'autenticazione a più fattori e la conduzione periodica di *audit* di sicurezza, contribuendo così a rafforzare l'adesione a normative settoriali come il GDPR.

72 ore ai sensi dell'art. 33 e, ove il rischio per i diritti degli interessati risulti elevato, alla comunicazione individuale *ex* art. 34; l'inadeguatezza delle misure tecniche e organizzative adottate, segnatamente in relazione all'art. 32, configura una responsabilità diretta del titolare, non attenuata dalla circostanza che il trattamento sia stato materialmente eseguito dal *provider*. Al contempo, la Direttiva NIS 2, nella misura in cui l'impresa rientri tra le entità essenziali, impone una segnalazione tempestiva all'autorità nazionale competente in materia di *cybersicurezza* secondo le modalità e le tempistiche previste dagli artt. 23 e 24, con obblighi di *reporting* che si aggiungono e non si sostituiscono alla notifica *privacy*. Sul versante settoriale, il Regolamento DORA richiede la classificazione dell'incidente secondo i criteri degli artt. 17 e 18, la segnalazione alle autorità di vigilanza competenti, segnatamente all'IVASS, nonché l'attivazione dei piani di continuità operativa e delle strategie di uscita contrattualmente predisposte. Inoltre, qualora il *provider* sia stato designato come fornitore *ICT* critico ai sensi dell'art. 31, l'incidente può determinare l'avvio di procedure ispettive da parte delle autorità europee di vigilanza nei confronti dello stesso fornitore.

In un siffatto scenario, la sola certificazione ISO/IEC 27001 del *provider* non vale a esimere l'impresa dalle proprie responsabilità: essa dovrebbe aver condotto una *due diligence* preventiva comprensiva di una DPIA ai sensi dell'art. 35 GDPR per il trattamento su larga scala di dati personali, aver negoziato clausole contrattuali che prevedano diritti di *audit* effettivi, *exit strategy* operative e cooperazione tempestiva in caso di incidente, e aver verificato la conformità delle misure di sicurezza del fornitore ai requisiti tanto dell'art. 28(3) GDPR quanto degli artt. 28-30 DORA. L'esempio mostra come la *compliance* sostanziale esiga non una sovrapposizione meccanica dei singoli adempimenti normativi, ma la loro integrazione organica in un sistema di *governance* unitario, presidiato dall'organo amministrativo, documentato e sottoposto a riesame periodico.

In ultima analisi, la regolazione del *cloud* in ambito assicurativo si configura come dovere di legalità sostanziale, punto di equilibrio tra innovazione e diritti fondamentali, tra libertà d'impresa e responsabilità sociale: è in questo equilibrio, nel quale gli standard tecnici svolgono un ruolo ausiliario ma non sostitutivo della norma, che si misura la capacità dell'ordinamento europeo di governare la transizione digitale

rafforzando, anziché comprimere, le garanzie della persona e l'affidabilità del mercato.