DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

La gestione degli incidenti ICT tra DORA e NIS2

Obblighi di trasparenza verso i clienti e profili reputazionali e risarcitori

Aprile 2026

Giulio Novellini, Partner, Portolano Cavallo

Giulio Novellini, Partner, Portolano Cavallo

Giulio Novellini

Giulio Novellini si occupa di Privacy, Cyber Security e Data Protection, Internet & Ecommerce e Nuove Tecnologie (quali Intelligenza Artificiale, Blockchain e Smart Contracts). Nel corso della sua esperienza professionale, ha assistito società nazionali e multinazionali occupandosi di contenzioso e compliance in materia di Protezione dei Dati Personali. Ha maturato un'esperienza particolare nella consulenza riguardante siti web e app, compliance online in materia di cookie, trattamento dei dati per finalità di Marketing, Ecommerce, trattamento transfrontaliero di dati personali e violazione dei dati personali.

Studio Legale

Portolano Cavallo

PORTOLANO CAVALLO

1. Introduzione: il quadro normativo europeo sulla resilienza digitale

Negli ultimi anni, il Legislatore europeo ha compiuto un progresso significativo nella regolamentazione della resilienza operativa digitale, riconoscendo che la crescente dipendenza dai sistemi tecnologici espone individui, imprese e infrastrutture critiche a rischi di portata sistemica. In questo contesto si inseriscono due strumenti normativi fondamentali: il Regolamento (UE) 2022/2554 (DORA - Digital Operational Resilience Act), applicabile dal 17 gennaio 2025, e la Direttiva (UE) 2022/2555 (NIS2), con termine di recepimento fissato al 17 ottobre 2024.

Sebbene entrambe le normative mirino al rafforzamento della cyber-resilienza nell'Unione europea, esse si distinguono per ambito applicativo, approccio metodologico e modalità di gestione e notifica degli incidenti ICT. Un punto di particolare interesse è rappresentato dagli obblighi di comunicazione verso i clienti in caso di incidente, nonché dalle ricadute reputazionali e dalle potenziali responsabilità risarcitorie.

La rilevanza pratica di tali questioni è dimostrata da episodi recenti: l'aggiornamento difettoso di CrowdStrike Falcon che nel luglio 2024 ha provocato l'interruzione di circa 8,5 milioni di sistemi Windows a livello globale[1]; l'attacco ransomware ai sistemi della ICBC nel novembre 2023, che ha paralizzato il ramo statunitense di negoziazione titoli dell'istituto[2]; l'attacco a Ion Group nel gennaio 2023, con impatto sulle operazioni di numerosi broker europei e statunitensi. Questi casi condividono un elemento ricorrente: il problema non è stato solo tecnico, ma anche comunicativo e legale.

Il 2025 ha rappresentato l'anno di svolta per la cyber-resilienza europea: con la piena operatività dei due regimi, le entità soggette operano all'interno di un quadro regolatorio pienamente vincolante. A partire dal 2026, tale quadro entra nella sua fase matura, imponendo standard elevati di preparazione, risposta e comunicazione. Per le entità finanziarie, in particolare, l'entrata a regime di DORA ha segnato il passaggio da un sistema basato su linee guida e raccomandazioni a un regime di obblighi direttamen-

1 Microsoft, Helping our customers through the CrowdStrike outage, luglio 2024, disponibile su: https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

2 Financial Times, ICBC hack disrupts US Treasury market trading, 10 novembre 2023, disponibile su: https://www.ft.com/content/ba19e0c2-0b1c-4b89-8b0e-81a4ff241e40.

vedi l'articolo online

te applicabili e assistiti da sanzioni, con implicazioni significative sul piano organizzativo, contrattuale e di governance.

2. Ambito applicativo: chi è soggetto a DORA e chi a NIS2

Il primo elemento di differenziazione tra i due regimi riguarda il perimetro soggettivo.

DORA si applica in via esclusiva al settore finanziario, disciplinando un ampio catalogo di soggetti: banche, imprese di investimento, istituti di pagamento e di moneta elettronica, imprese di assicurazione e riassicurazione, gestori di fondi, controparti centrali, depositari centrali di titoli, sedi di negoziazione, fornitori di servizi di crowdfunding e per le cripto-attività e, infine, i fornitori terzi di servizi ICT critici. La ratio è chiara: il sistema finanziario è un'infrastruttura critica la cui instabilità può generare effetti sistemici a catena sull'intera economia.

NIS2 adotta un approccio orizzontale, classificando i soggetti in entità essenziali (tra cui energia, trasporti, settore bancario, sanità, infrastrutture digitali e pubblica amministrazione) ed entità importanti (tra cui servizi postali, gestione dei rifiuti, fornitori di servizi digitali e ricerca).

La distinzione tra entità essenziali ed entità importanti non è meramente classificatoria, ma si riflette in un regime sanzionatorio differenziato. Per le entità essenziali, NIS2 prevede sanzioni amministrative pecuniarie fino a un massimo di almeno 10 milioni di euro o del 2% del fatturato mondiale annuo totale dell'esercizio precedente, se superiore; per le entità importanti, la soglia è fissata a un massimo di almeno 7 milioni di euro o dell'1,4% del fatturato mondiale annuo totale. Tale differenziazione riflette la diversa criticità sistemica delle due categorie e il diverso livello di aspettativa in termini di maturità delle misure di sicurezza.

Sul piano soggettivo, la Direttiva si applica di regola alle medie e grandi imprese ai sensi della raccomandazione 2003/361/CE della Commissione, escludendo in linea di principio le micro e piccole imprese. Tuttavia, sono previste eccezioni significative: indipendentemente dalle dimensioni, rientrano nell'ambito applicativo di NIS2 le seguenti categorie di soggetti:

- i fornitori di reti di comunicazione elettronica pubbliche;
- i prestatori di servizi fiduciari;
- i registri dei nomi di dominio di primo livello e i fornitori di servizi DNS;
- le entità identificate come critiche dagli Stati membri.

Va segnalato che, in virtù del principio di specialità (art. 4 NIS2), i soggetti finanziari già sottoposti a DORA sono esclusi dall'ambito applicativo di NIS2 per quanto concerne i requisiti di sicurezza delle reti e dei sistemi informativi. La Commissione europea ha confermato tale impostazione, e le ESAs hanno chiarito che le entità finanziarie soggette a DORA non sono tenute a effettuare una doppia notifica degli incidenti ICT, fermo restando l'obbligo delle autorità competenti settoriali di trasmettere le informazioni rilevanti ai CSIRT nazionali e all'ENISA. Permangono tuttavia zone grigie: si pensi al caso di un gruppo bancario che controlli entità operanti in settori soggetti a NIS2 ma estranei al perimetro DORA, ovvero ai fornitori terzi di servizi ICT che prestino servizi sia a entità finanziarie soggette a DORA sia a operatori soggetti a NIS2. In tali ipotesi, il gruppo o il fornitore deve conformarsi a entrambi i regimi, con evidenti complessità di coordinamento che suggeriscono l'opportunità di linee guida congiunte ESAs-ENISA.

3. La gestione degli incidenti ICT: struttura e obblighi a confronto

3.1 *Il regime DORA*

DORA dedica ampio spazio alla gestione degli incidenti ICT, con una disciplina particolarmente articolata e prescrittiva. Le entità finanziarie sono tenute a:

- Istituire e mantenere un processo di gestione degli incidenti ICT che consenta di rilevare, gestire e notificare tali incidenti in modo strutturato.
- Classificare gli incidenti in base a criteri predefiniti, tra cui l'impatto sui servizi, il numero di clienti interessati, la criticità dei sistemi colpiti, la portata geografica e le perdite economiche.
- Notificare gli incidenti gravi alle autorità competenti secondo un meccanismo articolato in tre fasi: una notifica iniziale (entro termini stringenti dalla classificazione dell'incidente), una rela-

zione intermedia e una relazione finale.

La Commissione europea e le autorità di vigilanza europee (ESAs - European Supervisory Authorities, ossia EBA, ESMA ed EIOPA) hanno lavorato allo sviluppo di standard tecnici di regolamentazione (RTS) e standard tecnici di attuazione (ITS) per la notifica degli incidenti, definendo i modelli uniformi, le scadenze e le soglie applicabili.

Merita particolare rilievo l'approccio di DORA riguardo alla notifica alle autorità: il regolamento prevede che, in caso di incidenti gravi, la notifica vada effettuata all'autorità competente dello Stato membro d'origine, che provvederà poi a trasmetterla alle autorità rilevanti (tra cui, se del caso, la Banca Centrale Europea e l'ENISA).

3.2 *Il regime NIS2*

NIS2 introduce anch'essa un sistema di notifica degli incidenti significativi, ma con una struttura in parte diversa. Il meccanismo di notifica si articola su quattro livelli:

- Preallarme (entro 24 ore dal momento in cui l'entità è venuta a conoscenza dell'incidente significativo): comunicazione iniziale volta a segnalare l'accadimento dell'incidente, indicando se si sospetta che sia causato da un atto illecito o possa avere un impatto transfrontaliero.
- Notifica dell'incidente (entro 72 ore): aggiornamento più completo con una prima valutazione dell'incidente, della sua gravità e del suo impatto.
- Relazione intermedia (su richiesta del CSIRT o dell'autorità competente): aggiornamento dello stato dell'incidente, con indicazione delle misure adottate e dell'evoluzione della situazione.
- Relazione finale (entro un mese dalla notifica): relazione dettagliata che descrive l'incidente, la sua natura, le cause radice, le misure adottate e, ove possibile, l'impatto transfrontaliero. In caso di incidente ancora in corso alla scadenza del termine di un mese, l'entità è tenuta a produrre un progress report e successivamente una relazione finale entro un mese dalla cessazione dell'incidente.

Le autorità destinatarie delle notifiche sono i CSIRT (Computer Security Incident Response Teams) nazionali o le autorità competenti designate da ciascuno Stato membro.

3.3 *Differenze chiave tra i due regimi*

Un confronto sistematico tra i due regimi evidenzia differenze significative lungo cinque dimensioni.

Sotto il profilo dell'ambito applicativo, DORA è settoriale (entità finanziarie), mentre NIS2 è orizzontale (pluralità di settori critici). Quanto alle soglie di notifica, DORA lavora con criteri prevalentemente quantitativi e dettagliati — numero di clienti, perdite finanziarie, durata dell'interruzione — mentre NIS2 combina criteri qualitativi e quantitativi senza raggiungere lo stesso grado di precisione.

La struttura temporale della notifica riflette questa differenza. DORA prevede notifica iniziale, relazione intermedia e relazione finale entro termini stringenti dalla classificazione dell'incidente. NIS2 prevede preallarme entro 24 ore, notifica entro 72 ore, relazione intermedia su richiesta e relazione finale entro un mese. Le due architetture condividono la logica della notifica progressiva, ma differiscono nelle scadenze e nel livello di prescrittività.

Sul versante delle autorità destinatarie, sotto DORA la notifica va all'autorità competente settoriale (in Italia, Banca d'Italia, Consob o IVASS, a seconda della tipologia di soggetto finanziario), con possibile trasmissione alla BCE e all'ENISA; sotto NIS2, il destinatario è il CSIRT nazionale o l'autorità NIS2 competente.

Un'ulteriore dimensione riguarda il regime sanzionatorio. DORA affida l'irrogazione delle sanzioni alle autorità di vigilanza settoriali nazionali (in Italia, Banca d'Italia, Consob e IVASS), secondo un modello consolidato di supervisione finanziaria. NIS2 prevede un sistema più frammentato, in cui ciascuno Stato membro designa una o più autorità competenti e uno o più CSIRT, con il rischio di eterogeneità nell'applicazione delle norme.

Sul piano degli standard tecnici, DORA opera attraverso RTS e ITS vincolanti emanati dalle ESAs (EBA, ESMA, EIOPA), garantendo un'armonizzazione massima a livello europeo. NIS2, in quanto direttiva, lascia maggiore discrezionalità agli Stati membri, con la conseguenza che il livello di prescrittività può

vedi l'articolo online

variare significativamente da uno Stato all'altro — circostanza che genera complessità per le entità operanti in più giurisdizioni. Con specifico riguardo al recepimento italiano, il D. Lgs. 4 settembre 2024, n. 138 ha confermato il ruolo centrale dell'Agenzia per la Cybersicurezza Nazionale (ACN) quale Autorità nazionale competente NIS2, con poteri di vigilanza, ispezione e sanzione, e ha designato il CSIRT Italia quale punto di riferimento per la ricezione delle notifiche. Le notifiche degli incidenti significativi devono essere effettuate attraverso la piattaforma digitale dell'ACN, secondo le tempistiche della Direttiva. Sul piano sanzionatorio, il decreto ha recepito le soglie massime previste dalla Direttiva e ha introdotto disposizioni in materia di responsabilità degli organi di gestione, prevedendo che i dirigenti apicali possano essere ritenuti personalmente responsabili in caso di violazione degli obblighi di supervisione, in linea con l'articolo 20 della Direttiva. Questo assetto istituzionale accentrato — che contrasta con il modello plurale adottato da altri Stati membri — presenta il vantaggio dell'uniformità di approccio, ma richiede che l'ACN disponga di risorse adeguate per un perimetro soggettivo significativamente più ampio rispetto alla previgente Direttiva NIS.

Quanto alla comunicazione verso i clienti, DORA introduce un obbligo esplicito di informazione dei clienti interessati, con indicazione delle misure di rimedio adottate; NIS2 prevede una comunicazione più generale, orientata a indicare agli utenti le misure che essi stessi possono adottare. Come si vedrà, questa differenza non è priva di conseguenze sul piano della responsabilità civile.

3.4 *Cenni comparativi: gli approcci extra-UE alla notifica degli incidenti cyber*

Il quadro normativo europeo non opera in un vuoto internazionale. Il riferimento più significativo è il framework della Securities and Exchange Commission (SEC) statunitense, che dal luglio 2023 impone alle società quotate l'obbligo di comunicare al mercato, mediante Form 8-K, qualsiasi incidente di cybersecurity ritenuto material entro quattro giorni lavorativi dalla determinazione della materialità. Il framework SEC si distingue dall'approccio europeo per tre profili: il destinatario primario è il mercato (non un'autorità di vigilanza o un CSIRT); il criterio di attivazione è la materialità, concetto giuridico indeterminato a differenza dei criteri più strutturati di DORA; il framework impone altresì obblighi di disclosure periodica sulla governance della cybersecurity nel Form 10-K. Meritano inoltre menzione il Prudential Standard CPS 234 dell'Australian Prudential Regulation Authority (APRA), che impone notifica entro 72 ore e requisiti stringenti di gestione del rischio ICT dei fornitori terzi, e il framework della Monetary Authority of Singapore (MAS), che prevede notifica entro un'ora per gli incidenti che compromettano servizi critici. Il confronto evidenzia una tendenza globale alla convergenza verso modelli di notifica tempestiva e strutturata, pur nella persistenza di differenze significative. Per le entità operanti a livello internazionale, questa pluralità di regimi impone processi di notifica sufficientemente flessibili da consentire l'adempimento simultaneo di obblighi parzialmente divergenti.

4. Gli obblighi di trasparenza verso i clienti

4.1 *La comunicazione ai clienti nel regime DORA*

Uno degli aspetti più rilevanti - e per certi versi innovativi - di DORA riguarda l'obbligo di comunicazione verso i clienti in caso di incidenti ICT gravi. L'articolo 19 del Regolamento stabilisce espressamente che, senza indebito ritardo, le entità finanziarie devono informare i propri clienti il cui impatto sugli interessi finanziari sia stato causato dall'incidente ICT grave, comunicando loro le misure adottate per attenuarne gli effetti negativi. Peraltro, lo stesso articolo prevede che, in caso di minaccia cyber significativa, le entità debbano informare i clienti potenzialmente colpiti delle misure di protezione che questi possono adottare autonomamente.

Questo obbligo si inserisce in un contesto in cui la clientela del settore finanziario è particolarmente vulnerabile: l'incidente ICT non si traduce solo in un disservizio tecnico, ma può causare danni economici diretti e immediati — correntisti impossibilitati ad accedere ai propri conti, investitori che non possono operare sui mercati, beneficiari di polizze che non ricevono i pagamenti dovuti.

4.2 *La comunicazione agli utenti nel regime NIS2*

NIS2 prevede anch'essa obblighi di comunicazione nei confronti degli utenti, ma con una formulazione più generale e meno specifica rispetto a DORA. L'articolo 23 della Direttiva prevede che, ove l'incidente significativo possa avere un impatto sulla fornitura di servizi agli utenti, l'entità interessata debba informare i destinatari dei propri servizi di tutti i provvedimenti o rimedi che questi ultimi possono adottare in risposta all'incidente.

Vi è quindi una differenza di enfasi: DORA si concentra sull'obbligo dell'entità di comunicare le proprie

misure di rimedio, mentre NIS2 orienta la comunicazione verso le misure che gli utenti stessi possono adottare. Questa diversa prospettiva riflette la differenza strutturale tra i due regimi: DORA disciplina entità che gestiscono direttamente risorse economiche dei clienti, mentre NIS2 copre settori in cui la relazione con l'utente finale è meno immediata.

4.3 *Il problema della tempestività e della completezza della comunicazione*

Un tema trasversale a entrambi i regimi — e di grande rilevanza pratica — è quello della tempestività e della completezza della comunicazione verso i clienti. Se la notifica alle autorità è scandita da termini precisi, la comunicazione ai clienti è soggetta a formule più elastiche: DORA (art. 19) prescrive che l'informazione avvenga "senza indebito ritardo", mentre NIS2 (art. 23) non fissa un termine specifico, limitandosi a prevedere l'obbligo di comunicazione ove l'incidente possa avere un impatto sulla fornitura dei servizi. Tali formulazioni, pur rispondendo all'esigenza di flessibilità, lasciano margini di incertezza applicativa che le entità devono gestire con particolare attenzione.

Le entità si trovano di fronte a una tensione tra la necessità di comunicare tempestivamente per rispettare gli obblighi normativi e tutelare la fiducia dei clienti, e l'esigenza di non diffondere informazioni incomplete nelle prime fasi dell'incidente. Questa tensione ha importanti implicazioni sia sotto il profilo reputazionale sia sotto quello della responsabilità civile.

5. I profili reputazionali: la gestione della crisi di immagine

5.1 *L'incidente ICT come evento reputazionale*

Un incidente ICT grave non è mai solo un evento tecnico: è, al contempo, un evento di comunicazione. Le modalità con cui l'entità gestisce la crisi - la tempestività della comunicazione, la chiarezza del messaggio, la dimostrazione di competenza e trasparenza - determinano in larga misura l'impatto reputazionale dell'incidente.

Nel settore finanziario, regolato da DORA, l'esposizione è particolarmente elevata: le entità finanziarie operano in un mercato fondato sulla fiducia, e un incidente ICT che comprometta la disponibilità dei servizi o la sicurezza dei dati può minare in modo duraturo tale fiducia, con effetti che vanno ben oltre il singolo episodio.

Un caso emblematico, per quanto antecedente all'entrata in vigore di DORA, è quello della banca britannica TSB. Nel 2018, una migrazione IT mal gestita ha reso inaccessibili i conti di circa 1,9 milioni di clienti per diversi giorni. La Financial Conduct Authority (FCA) ha comminato una sanzione di circa £ 48,6 milioni, ma il costo reputazionale è risultato di gran lunga superiore: TSB ha perso quote di mercato significative, ha rimborsato ai clienti oltre 32 milioni di sterline e ha visto il proprio CEO dimettersi[3] [4]. Il caso dimostra come un incidente ICT, in assenza di una comunicazione adeguata e tempestiva, possa trasformarsi in una crisi istituzionale.

5.2 *Il ruolo degli obblighi di notifica nella gestione reputazionale*

Paradossalmente, gli obblighi di notifica possono rivelarsi uno strumento di gestione reputazionale. La trasparenza obbligatoria, se gestita correttamente, permette all'entità di controllare la narrativa dell'incidente: comunicare per prima e fornire informazioni accurate è quasi sempre preferibile rispetto allo scenario in cui la notizia emerge da fonti esterne.

Il concetto di "narrative control" — la capacità dell'entità di orientare la percezione pubblica dell'incidente attraverso una comunicazione proattiva e tempestiva — assume un rilievo strategico di primo piano. L'entità che comunica per prima e in modo trasparente sottrae spazio alla speculazione mediatica e alle ricostruzioni approssimative. Al contrario, il silenzio o la comunicazione tardiva creano un vuoto informativo rapidamente colmato da fonti esterne, con effetti amplificativi sul danno reputazionale.

Un esempio significativo è la risposta di CrowdStrike durante l'outage globale del luglio 2024: la società ha adottato una strategia di comunicazione caratterizzata dalla pubblicazione tempestiva di aggiornamenti tecnici dettagliati, dalla creazione di un hub dedicato alla remediation e dalla trasparenza sulle cause e sulle misure correttive. Questo approccio ha contribuito a contenere il danno reputazionale

3 House of Commons Treasury Committee, IT Failures in the Financial Services Sector, aprile 2023, disponibile su: https://committees.parliament.uk/work/6993/it-failures-in-the-financial-services-sector/.

4 Financial Conduct Authority (FCA), Final Notice - TSB Bank plc, 20 dicembre 2022, disponibile su: https://www.fca.org.uk/publication/final-notices/tsb-bank-plc-2022.pdf.

rispetto alla portata tecnica dell'evento, dimostrando che la qualità della comunicazione di crisi può costituire un fattore di mitigazione almeno parzialmente indipendente dalla gravità dell'incidente [5].

5.3 *Le specificità del regime DORA sotto il profilo reputazionale*

DORA introduce un elemento ulteriore di complessità reputazionale attraverso il meccanismo di supervisione dei fornitori terzi di servizi ICT critici. Se l'incidente è originato da un fornitore terzo - si pensi a un provider di servizi cloud o a un fornitore di infrastrutture IT - il problema della responsabilità (e della narrazione pubblica) diventa più articolato. L'entità finanziaria, che rimane responsabile in ultima istanza verso i propri clienti e le autorità di vigilanza, deve essere in grado di comunicare efficacemente anche quando l'incidente non è direttamente nella propria sfera di controllo.

I casi Ion Group (gennaio 2023) e CrowdStrike Falcon (luglio 2024) sono istruttivi: in entrambi, le entità finanziarie si sono trovate a dover comunicare ai propri clienti interruzioni di servizio la cui causa risiedeva interamente nella sfera di un fornitore terzo, senza poter fornire tempistiche certe di ripristino[5]. Questi episodi evidenziano l'urgenza di definire, già in sede contrattuale, protocolli di comunicazione coordinata tra entità finanziarie e fornitori terzi critici, con dirette implicazioni sulla risk allocation contrattuale.

5.4 *Le specificità del regime NIS2 sotto il profilo reputazionale*

Per i soggetti sottoposti a NIS2, il rischio reputazionale è amplificato dalla pubblicità delle sanzioni. NIS2 prevede esplicitamente la possibilità per le autorità competenti di rendere pubblica la violazione degli obblighi normativi da parte delle entità, con la conseguenza che una gestione inadeguata degli incidenti - inclusa una notifica tardiva o incompleta - può tradursi in una sanzione formale resa pubblica, con effetti devastanti sull'immagine dell'organizzazione.

5 CrowdStrike, Falcon Content Update Remediation and Guidance Hub, luglio 2024, disponibile su: https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/.

6. I profili risarcitori: responsabilità civile e tutela dei clienti

6.1 *Il rapporto tra violazione normativa e responsabilità civile*

La questione della responsabilità civile da incidente ICT è, allo stato attuale, uno dei temi più controversi e ancora privi di soluzione definitiva nell'ordinamento europeo. Né DORA né NIS2 disciplinano direttamente la responsabilità civile delle entità verso i terzi danneggiati: entrambi i regimi si concentrano sugli obblighi di natura pubblicistica (notifica alle autorità, adozione di misure tecniche e organizzative) e sulle sanzioni amministrative in caso di violazione.

Tuttavia, la violazione degli obblighi previsti da DORA e NIS2 può rilevare sul piano della responsabilità civile in almeno due modi, trovando il proprio fondamento nelle norme generali dell'ordinamento nazionale: nell'ambito della responsabilità extracontrattuale, ai sensi dell'art. 2043 c.c. (risarcimento per fatto illecito), ove la violazione degli obblighi normativi integri un comportamento colposo produttivo di danno ingiusto; nell'ambito della responsabilità contrattuale, ai sensi dell'art. 1218 c.c. (responsabilità del debitore), ove l'inadempimento degli obblighi di sicurezza e di comunicazione si inserisca nel rapporto contrattuale tra l'entità e i propri clienti.

In concreto, la violazione normativa può rilevare sotto un duplice profilo: come elemento di accertamento della colpa dell'entità, ove questa non abbia adottato le misure prescritte o non abbia comunicato tempestivamente ai clienti; e ai fini della causalità, ove la tempestiva comunicazione avrebbe consentito ai clienti di adottare misure protettive idonee a ridurre o evitare il danno (si pensi al caso di credenziali compromesse di cui i clienti vengano informati tardivamente).

6.2 *I potenziali danni risarcibili*

Sul piano pratico, i danni risarcibili in connessione con un incidente ICT possono essere di varia natura.

La categoria più immediata è quella dei danni patrimoniali diretti: transazioni non autorizzate effettuate da terzi che hanno sfruttato la compromissione dei sistemi, ovvero impossibilità di accedere ai propri fondi durante un'interruzione del servizio.

Merita infine attenzione il danno da ritardata comunicazione: il pregiudizio causato non dall'incidente

vedi l'articolo online

in sé, ma dalla mancata o tardiva informazione dei clienti, che ha impedito loro di adottare misure protettive tempestive (blocco credenziali, sostituzione carte compromesse, monitoraggio rafforzato dei conti). In questi casi, il nesso causale tra omissione comunicativa e danno può essere ricostruito con sufficiente precisione, aprendo uno spazio autonomo di responsabilità civile.

6.3 *L'interazione con il GDPR*

Un elemento di complessità ulteriore è l'interazione tra gli obblighi di notifica degli incidenti ICT (DORA/NIS2) e quelli previsti dal GDPR in materia di violazioni dei dati personali.

Molto spesso, un incidente ICT grave è anche una violazione dei dati personali ai sensi dell'art. 4, n. 12 del GDPR, con conseguente obbligo di notifica al Garante entro 72 ore e, ove sussista un rischio elevato, di comunicazione agli interessati senza indebito ritardo.

Questa sovrapposizione — ICT incident notification e data breach notification — crea complessità operativa significativa, richiedendo il coordinamento di flussi di notifica distinti verso autorità diverse con tempistiche talvolta disallineate.

Sul piano risarcitorio, la compresenza del regime GDPR (art. 82) arricchisce il panorama delle pretese avanzabili dai clienti danneggiati — anche con riguardo al danno non patrimoniale, come chiarito dalla Corte di Giustizia nella sentenza del 4 maggio 2023, causa C-300/21, Österreichische Post[6] — generando al contempo un problema di "doppio binario" sanzionatorio: un medesimo incidente ICT che integri anche una violazione dei dati personali può esporre l'entità a sanzioni cumulative sotto DORA o NIS2 per omessa o tardiva notifica dell'incidente ICT e sotto il GDPR per omessa o tardiva notifica della violazione dei dati personali al Garante.

6.4 *L'azione collettiva come rischio amplificato*

Un ulteriore profilo di rischio è quello delle azioni collettive. Con l'entrata in vigore del D. Lgs. 28 marzo 2023, n. 28, di attuazione della Direttiva (UE) 2020/1828 sulle azioni rappresentative, le organizzazioni dei consumatori dispongono di strumenti più efficaci per promuovere azioni risarcitorie collettive, con potenziali esposizioni risarcitorie tali da amplificare significativamente l'impatto economico degli incidenti che interessino un numero elevato di clienti.

Il panorama europeo offre già segnali significativi: in Germania, a seguito della violazione dei dati di Deutsche Wohnen, sono state avviate azioni di classe[7], anche alla luce della sentenza della Corte di Giustizia UE del 5 dicembre 2023 (causa C-807/21) sulla responsabilità diretta delle persone giuridiche per violazioni GDPR; in Irlanda, la sanzione da 1,2 miliardi di euro a Meta ha stimolato il dibattito su azioni rappresentative coordinate[8]. In Italia, merita menzione il provvedimento del Garante nei confronti di UniCredit S.p.A. (provvedimento n. 99 del 10 giugno 2020) per un data breach che aveva coinvolto circa 762.000 clienti. Con il consolidamento degli strumenti del D. Lgs. n. 28/2023, le entità finanziarie italiane devono considerare il rischio di azioni collettive come una componente concreta della loro esposizione complessiva.

6.5 *I profili assicurativi: le polizze cyber come strumento di mitigazione del rischio*

Un aspetto di crescente rilevanza pratica è rappresentato dalle coperture assicurative cyber, che possono costituire uno strumento significativo di mitigazione dell'esposizione risarcitoria e sanzionatoria, coprendo — a seconda della struttura contrattuale — i costi di risposta all'incidente, le perdite da interruzione dell'attività, le spese legali e le esposizioni verso terzi. Tuttavia, l'evoluzione normativa e l'incremento della frequenza degli incidenti pongono sfide rilevanti in termini di adeguatezza delle coperture e di portata delle esclusioni contrattuali.

Tra le esclusioni contrattuali di maggiore rilevanza si segnala la "war exclusion", che esclude dalla copertura i danni derivanti da atti di guerra. L'applicabilità di tale clausola agli attacchi informatici attri-

6 Corte di Giustizia dell'Unione Europea, sentenza del 4 maggio 2023, causa C-300/21, UI c. Österreichische Post AG, ECLI:EU:C:2023:370, disponibile su: https://curia.europa.eu/juris/document/document.jsf?docid=273284.

7 Berliner Beauftragte für Datenschutz und Informationsfreiheit (BInBDI), decisione nei confronti di Deutsche Wohnen SE, settembre 2021, comunicato stampa disponibile su: https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/pressemitteilungen/detail/article/berliner-datenschutzbeauftragte-verhaengt-bussgeld-gegen-deutsche-wohnen-se.

8 Data Protection Commission (DPC) Ireland, decisione nei confronti di Meta Platforms Ireland Limited, maggio 2023, comunicato stampa disponibile su: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-conclusion-of-inquiry-into-meta-ireland.

buiti ad attori statali (state-sponsored attacks) è una delle questioni più dibattute nel diritto assicurativo contemporaneo. Nel caso Merck & Co. v. Ace American Insurance Co., relativo all'attacco NotPetya del 2017, la Superior Court del New Jersey (confermata in appello nel 2023) ha rigettato l'eccezione degli assicuratori, ritenendo che la formulazione tradizionale della war exclusion non potesse essere estesa agli attacchi informatici senza adeguata riformulazione contrattuale. Tale pronuncia ha indotto i principali sindacati dei Lloyd's di Londra a introdurre, dal 2023, clausole di esclusione specifiche per gli attacchi cyber state-sponsored.

Un'ulteriore area di criticità riguarda le esclusioni per eventi sistemici o catastrofici: le polizze cyber tendono a limitare la copertura per incidenti che colpiscano simultaneamente una pluralità di assicurati, in ragione del rischio di correlazione delle perdite. Per le entità finanziarie soggette a DORA, questa limitazione è particolarmente rilevante alla luce dell'elevata concentrazione del mercato dei fornitori terzi di servizi ICT critici. L'integrazione della copertura assicurativa cyber nel framework complessivo di gestione del rischio ICT rappresenta pertanto un elemento di prudente governance, complementare rispetto alle misure tecniche e organizzative prescritte dalla normativa. Le entità sono chiamate a valutare periodicamente l'adeguatezza delle proprie coperture alla luce dell'evoluzione delle minacce, delle esclusioni contrattuali e dei requisiti regolatori.

7. Governance degli incidenti: implicazioni pratiche per le entità

7.1 *La centralità del piano di risposta agli incidenti*

Tanto DORA quanto NIS2 richiedono piani strutturati per la risposta agli incidenti ICT, effettivamente operativi e periodicamente testati. L'esistenza di un piano adeguato e strutturato rappresenta un elemento di difesa sia sul piano regolatorio sia su quello della responsabilità civile.

Il piano deve includere procedure chiare per la comunicazione verso i clienti, con individuazione dei soggetti responsabili, dei canali e dei messaggi predefiniti per le diverse tipologie di incidente. La predisposizione di questi strumenti in anticipo è ciò che distingue un'entità capace di gestire una crisi in modo credibile.

Un elemento qualificante del regime DORA è l'obbligo, per le entità finanziarie di rilevanza sistemica, di condurre periodicamente test avanzati di resilienza mediante Threat-Led Penetration Testing (TLPT), secondo gli articoli 26 e 27 del Regolamento e il framework TIBER-EU. Tali test, che simulano scenari di attacco realistici, costituiscono uno strumento essenziale per verificare l'effettiva capacità di rilevazione e risposta dell'entità, rafforzando la credibilità complessiva del piano di risposta agli incidenti.

7.2 *Il ruolo del Consiglio di Amministrazione*

DORA attribuisce al consiglio di amministrazione la responsabilità ultima nella definizione della strategia di rischio ICT, incluse le politiche di gestione degli incidenti. NIS2 si spinge oltre sul piano della responsabilizzazione individuale: l'articolo 20 prevede che gli organi di gestione approvino le misure di gestione del rischio di cybersecurity, ne supervisionino l'attuazione e possano essere ritenuti responsabili per le violazioni. La medesima norma impone altresì obblighi formativi specifici in materia di cybersecurity per i membri degli organi di gestione.

Questa responsabilizzazione degli organi apicali implica che una gestione inadeguata degli incidenti ICT — inclusa la mancata adozione di piani di risposta adeguati o l'omessa supervisione delle misure di sicurezza — può esporre i singoli amministratori a responsabilità per violazione dei doveri di diligenza, con conseguenze che si estendono dal piano sanzionatorio a quello della responsabilità civile verso la società e verso i terzi danneggiati.

7.3 *La gestione contrattuale del rischio ICT nei rapporti con i fornitori terzi*

La crescente dipendenza delle entità finanziarie — e, più in generale, delle entità soggette a NIS2 — da fornitori terzi di servizi ICT rende la dimensione contrattuale un presidio essenziale nella gestione del rischio di incidenti. DORA disciplina esplicitamente, all'articolo 30, i requisiti contrattuali minimi che le entità finanziarie devono prevedere nei contratti con i fornitori terzi di servizi ICT, con particolare rigore per i fornitori qualificati come critici. In questa prospettiva, è fondamentale che i contratti con i fornitori terzi ICT includano clausole specifiche su almeno quattro profili chiave:

- Obblighi di notifica tempestiva degli incidenti: il fornitore deve essere contrattualmente tenuto a comunicare all'entità cliente, entro termini predefiniti e stringenti, qualsiasi incidente ICT che possa avere un impatto sui servizi forniti, consentendo all'entità di adempiere a propria volta ai

propri obblighi di notifica verso le autorità competenti e verso i clienti finali.

- Service Level Agreement (SLA) con penali per mancato rispetto dei tempi di ripristino: la definizione di livelli di servizio misurabili e di meccanismi di penale in caso di inadempimento costituisce uno strumento di incentivazione contrattuale alla resilienza operativa del fornitore e, al contempo, un parametro oggettivo per la valutazione delle responsabilità in caso di incidente.
- Diritto di audit del cliente sulle misure di sicurezza del fornitore: l'entità deve riservarsi il diritto di verificare, direttamente o tramite terzi indipendenti, l'adeguatezza delle misure tecniche e organizzative adottate dal fornitore, inclusa la capacità di risposta agli incidenti.
- Allocazione contrattuale del rischio di sanzioni regolatorie: nei casi in cui un incidente originato presso il fornitore determini l'irrogazione di sanzioni all'entità cliente, è opportuno prevedere meccanismi di manleva o di contribuzione che riflettano l'effettiva ripartizione delle responsabilità.

La predisposizione di un assetto contrattuale solido rappresenta un elemento di difesa sostanziale sia sul piano della gestione operativa della crisi sia su quello della limitazione delle esposizioni risarcitorie e sanzionatorie.

8. Conclusioni: verso un sistema integrato di gestione degli incidenti

L'analisi comparata dei regimi DORA e NIS2 evidenzia un quadro normativo in rapida evoluzione, caratterizzato da ambizioni elevate in termini di resilienza digitale ma anche da significativa complessità applicativa[9].

Gli obblighi di trasparenza verso i clienti rappresentano un elemento di grande rilevanza pratica. La loro gestione efficace non è semplicemente una questione di compliance: è un fattore determinante per la tutela della fiducia, la protezione della reputazione e la limitazione delle esposizioni risarcitorie.

Per i professionisti legali, le priorità operative sono chiare: aggiornare i piani di risposta agli incidenti; strutturare e testare le procedure di comunicazione verso i clienti; rivedere i contratti con i fornitori ICT per una corretta allocazione del rischio; monitorare l'evoluzione della giurisprudenza e delle prassi sanzionatorie.

Guardando alle prospettive future, il quadro normativo delineato da DORA e NIS2 è destinato a consolidarsi e ad arricchirsi attraverso almeno tre direttrici, in un contesto in cui il legislatore europeo continua ad ampliare il perimetro della regolamentazione della resilienza digitale — come testimoniato dall'adozione del Regolamento (UE) 2024/2847 (Cyber Resilience Act), la cui interazione con DORA e NIS2 richiederà un'attenta opera di coordinamento interpretativo e applicativo.

Un profilo di crescente rilevanza è rappresentato dall'interazione tra i regimi DORA e NIS2 e il Regolamento (UE) 2024/1689 (AI Act). La progressiva integrazione di componenti di intelligenza artificiale nei sistemi ICT del settore finanziario e delle infrastrutture critiche — dai modelli di scoring creditizio ai sistemi di rilevazione delle frodi, dai processi automatizzati di trading algoritmico alla gestione automatizzata delle reti energetiche — pone interrogativi rilevanti in ordine alla qualificazione degli incidenti originati da malfunzionamenti o vulnerabilità di tali componenti. In particolare, ove un sistema di IA classificato ad alto rischio ai sensi dell'AI Act sia parte integrante dell'infrastruttura ICT di un'entità soggetta a DORA o a NIS2, un suo malfunzionamento potrebbe configurare al contempo un incidente ICT rilevante ai fini della notifica e un evento rilevante ai sensi degli obblighi di monitoraggio post-commercializzazione previsti dall'AI Act, con conseguente necessità di coordinare flussi informativi e obblighi di segnalazione verso autorità diverse.

La prima è l'evoluzione della prassi sanzionatoria delle autorità competenti: le prime decisioni in materia di violazione degli obblighi di notifica e di gestione degli incidenti stanno definendo i parametri concreti di applicazione delle norme, contribuendo a chiarire le aree di incertezza interpretativa che caratterizzano questa fase iniziale del nuovo regime regolatorio.

La seconda direttrice è il ruolo della giurisprudenza nel definire i confini della responsabilità civile da incidente ICT: le corti nazionali ed europee saranno chiamate a pronunciarsi su questioni cruciali quali

9 Finocchiaro G., Cyber Security Law. La regolamentazione della sicurezza informatica, in Contratto e impresa, 2024; Tosoni L., The Impact of the NIS2 Directive and DORA on Cybersecurity Governance, in European Journal of Risk Regulation, 2024; Panetta R., Cybersicurezza. Nuovi assetti regolatori e profili di responsabilità, Giuffrè, 2024; ENISA, NIS2 Directive - Implementing Guidance, 2024, disponibile su: https://www.enisa.europa.eu.

vedi l'articolo online

il nesso causale tra omissione comunicativa e danno, la quantificazione del danno da ritardata informazione, l'applicabilità dei principi di ne bis in idem in caso di sanzioni cumulative e la ripartizione della responsabilità tra entità finanziarie e fornitori terzi ICT.

La terza direttrice, infine, è la progressiva maturazione di un approccio integrato alla gestione del rischio digitale, che combini compliance normativa, gestione della comunicazione di crisi e presidio contrattuale dei rapporti con i fornitori terzi in un quadro unitario e coerente.

In questa prospettiva, appare auspicabile, de iure condendo, l'istituzione di un meccanismo di notifica unificato — un "single entry point" — per gli incidenti che ricadano simultaneamente nell'ambito applicativo di DORA, NIS2 e GDPR. L'attuale frammentazione dei flussi di notifica verso autorità di vigilanza finanziaria, CSIRT nazionali e autorità di protezione dei dati personali impone alle entità un onere operativo significativo e genera il rischio di disallineamenti temporali e contenutistici tra le diverse comunicazioni. Un punto di ingresso unico, che consenta la trasmissione di una notifica integrata successivamente instradata alle autorità competenti ratione materiae, ridurrebbe la complessità operativa, favorirebbe la coerenza delle informazioni trasmesse e consentirebbe alle autorità stesse una visione più tempestiva e completa degli incidenti a rilevanza trasversale.

Le entità che sapranno anticipare queste evoluzioni — investendo nella formazione degli organi di governance, nella strutturazione dei processi di risposta e nella qualità dei presidi contrattuali — disporranno di un vantaggio competitivo significativo in un contesto regolatorio e di mercato in cui la resilienza digitale è ormai un fattore determinante di affidabilità e di reputazione.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it