DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

L'information sharing nel regime DORA

Un nuovo paradigma di collaborazione regolamentata tra cybersecurity e data protection

30 Giugno 2025

Sergio Visalli, Senior Associate, Alma LED

Sergio Visalli, Senior Associate, Alma LED

1. Introduzione

La crescente digitalizzazione del settore finanziario ha reso le istituzioni sempre più vulnerabili a minacce informatiche complesse e transfrontaliere. Tale evoluzione ha imposto al legislatore europeo di elaborare un quadro normativo uniforme in grado di assicurare la resilienza operativa digitale degli operatori, favorendo al contempo la cooperazione tra enti pubblici e privati. In tale contesto si inserisce il Regolamento (UE) 2022/2554 (*Digital Operational Resilience Act*, c.d. DORA), che stabilisce requisiti armonizzati per la gestione del rischio ICT nel settore finanziario. Tra le sue disposizioni più innovative si distingue l'articolo 45, che disciplina lo scambio di informazioni e analisi relative alle minacce informatiche.

L'art. 45 DORA, combinando esigenze di sicurezza informatica, tutela dei dati personali e rispetto delle regole di concorrenza, rappresenta un punto di svolta nell'approccio regolamentare europeo: da una logica meramente difensiva a un modello di condivisione fiduciaria e regolamentata dell'informazione, finalizzato a rafforzare la resilienza collettiva del sistema.

Il presente articolo intende analizzare il contenuto, la *ratio* e le implicazioni pratiche dell'art. 45 DORA, evidenziando le connessioni sistemiche con gli altri pilastri della resilienza digitale (gestione del rischio, *incident reporting*, terze parti ICT e testing), nonché le interazioni e le potenziali frizioni con la normativa in materia di protezione dei dati personali (GDPR) e con la Direttiva NIS2.

2. La governance europea della resilienza digitale: il quadro introdotto dal Regolamento DORA

Il Regolamento DORA si applica a un'ampia gamma di entità del settore finanziario, tra cui banche, assicurazioni, società di gestione, imprese di investimento, prestatori di servizi per le cripto-attività, istituti di pagamento e di moneta elettronica nonché fornitori terzi di servizi ICT rilevanti. Obiettivo dichiarato è quello di garantire che tutte le entità finanziarie possano continuare ad operare anche in presenza di gravi disservizi o attacchi informatici, grazie a presidi di prevenzione, gestione, recupero e cooperazione.

La resilienza operativa è articolata in cinque pilastri:

- gestione del rischio ICT;
- segnalazione degli incidenti informatici;
- test di resilienza operativa;
- gestione del rischio legato ai fornitori terzi;
- meccanismi di comunicazione e condivisione delle informazioni.

La disciplina della condivisione informativa (cd. "*information sharing*") si colloca all'incrocio tra il pilastro della gestione del rischio e quello della cooperazione settoriale, configurandosi come un elemento chiave per la creazione di un ecosistema finanziario europeo più sicuro, trasparente e reattivo.

3. Il contenuto normativo dell'art. 45 DORA: struttura e finalità

La crescente complessità e sofisticazione delle minacce informatiche nel settore finanziario richiede una risposta normativa altrettanto strutturata, che ponga al centro la collaborazione attiva tra operatori. In questa prospettiva, il Considerando (32)[1] DORA individua con chiarezza il fondamento logico e funzionale della disciplina di cui all'art. 45. Secondo tale Considerando, "*la validità delle misure di individuazione e prevenzione dei rischi informatici dipende in larga misura da una costante condivisione delle analisi delle minacce e delle vulnerabilità tra le entità finanziarie*". La condivisione di informazioni (c.d. *threat intelligence sharing*) non è dunque solo una buona prassi tecnica, bensì diventa una condizione

1 Il Considerando (32) DORA prevede che: "*Di fronte ai rischi informatici che si fanno sempre più complessi e sofisticati, la validità delle misure di individuazione e prevenzione dei rischi informatici dipende in larga misura da una costante condivisione delle analisi delle minacce e delle vulnerabilità tra le entità finanziarie. La condivisione delle informazioni contribuisce a creare una maggiore consapevolezza delle minacce informatiche. Ciò a sua volta accresce la capacità delle entità finanziarie di impedire che le minacce informatiche si trasformino in incidenti concreti connessi alle TIC e consente alle entità finanziarie di arginare in maniera più efficace l'impatto degli incidenti connessi alle TIC e di effettuare un ripristino più rapido. In assenza di orientamenti a livello di Unione, numerosi fattori, tra cui in particolare l'incertezza sulla compatibilità con le norme in materia di protezione dei dati, antitrust e responsabilità, hanno apparentemente ostacolato la condivisione dei dati.*".

abilitante per garantire la resilienza collettiva del sistema. In tal senso, come chiarito da Banca d'Italia, la disciplina DORA, tra le altre cose, promuove meccanismi volontari di condivisione delle informazioni nell'ambito dell'Unione europea "*volti ad aiutare la comunità del settore finanziario a prevenire le minacce informatiche e a rispondervi collettivamente, contenendo rapidamente la diffusione dei rischi informatici e impedendo il potenziale contagio tramite i canali finanziari*"[2].

Tale attività, invero, oltre a favorire la consapevolezza situazionale in merito agli attacchi in corso o potenziali, consente alle entità finanziarie di prevenire l'*escalation* degli eventi dannosi, arginare gli impatti di incidenti legati alle TIC, ed effettuare tempestive azioni di *recovery*. Tuttavia, l'assenza di un quadro giuridico armonizzato a livello dell'Unione ha sinora ostacolato queste iniziative: le incertezze in merito alla compatibilità della condivisione con la normativa in materia di protezione dei dati personali, concorrenza e responsabilità civile hanno frenato molte iniziative collaborative spontanee.

Per rispondere a questa esigenza sistemica, l'articolo 45 DORA si inserisce nella logica di rafforzamento della resilienza operativa digitale del settore finanziario europeo, attraverso la regolazione di un meccanismo volontario e fiduciario di condivisione delle informazioni sulle minacce informatiche tra le entità finanziarie. L'approccio normativo adottato mira a conciliare le esigenze di sicurezza collettiva con quelle di tutela della riservatezza e dei dati personali, nonché con il rispetto delle regole sulla concorrenza.

Il primo comma dell'articolo 45 autorizza espressamente le entità finanziarie a scambiarsi reciprocamente informazioni e analisi su minacce e vulnerabilità *cyber*, a condizione che tale attività rispetti tre presupposti cumulativi:

a) sia finalizzata a rafforzare la resilienza operativa digitale (ad esempio accrescendo la consapevolezza sulle minacce informatiche, migliorando le capacità di difesa, individuazione, risposta e ripristino);

b) si svolga entro "comunità fidate" di entità finanziarie;

2 Cfr. Comunicazione di Banca d'Italia del 30 dicembre 2025 rivolta agli intermediari vigilati in ambito DORA, di cui al seguente link: https://www.bancaditalia.it/media/notizia/regolamento-dora-comunicazione-al-mercato/

vedi l'articolo online

c) sia regolata da meccanismi di condivisione disciplinati da norme di condotta rispettose del GDPR, della riservatezza dell'attività economica e delle *policy* in materia di concorrenza.

Il concetto di "comunità fidate" non è esplicitamente definito nel DORA, ma implica la preesistenza di relazioni di fiducia, basate su criteri di adesione, trasparenza, protezione dei dati e affidabilità degli attori coinvolti. La fiducia reciproca, infatti, è il presupposto per uno scambio efficace di informazioni sensibili che, se divulgate impropriamente, potrebbero generare rischi sistemici, violazioni regolamentari o impatti reputazionali.

Il secondo comma specifica che i meccanismi di condivisione devono definire le condizioni di partecipazione, l'eventuale coinvolgimento delle autorità pubbliche (specificando la loro veste) e dei fornitori terzi di servizi TIC, nonché gli strumenti operativi a supporto, come le piattaforme informatiche.

Il terzo comma introduce un ulteriore adempimento: le entità finanziarie sono tenute a notificare alle autorità competenti la loro partecipazione a tali meccanismi, sia in fase di adesione sia in caso di recesso, quando quest'ultimo abbia effetto. Si tratta di una forma di *accountability* istituzionale che consente alle autorità di mappare e monitorare l'effettiva operatività dei meccanismi collaborativi.

L'art. 45, infine, si lega strettamente al Considerando (34)[3] DORA, il quale sottolinea la necessità di istituire a livello dell'Unione meccanismi volontari di condivisione in ambienti sicuri, per aiutare il settore finanziario a prevenire e contenere rapidamente i rischi informatici, evitando effetti di contagio attraverso i canali finanziari.

4. Le connessioni con la disciplina sulla comunicazione delle crisi (art. 14 DORA)

L'articolo 14 del DORA, rubricato "*Comunicazioni*", introduce un ulteriore pilastro del sistema di resilienza operativa digitale fondato sulla trasparenza e sulla tempestività nella gestione degli incidenti connessi alle tecnologie dell'informazione e della comunicazione (TIC). Esso si colloca in un rapporto di complementarità con l'articolo 45, che disciplina i meccanismi volontari di condivisione delle informazioni sulle minacce informatiche. Mentre l'articolo 45 promuove lo scambio orizzontale di conoscenze tra entità finanziarie, in logica collaborativa, l'articolo 14 impone obblighi verticali di comunicazione verso *stakeholder* interni ed esterni, secondo una logica di *accountability* organizzativa.

Detta disposizione normativa prevede due livelli di azione: da un lato, l'elaborazione di piani di comunicazione delle crisi, dall'altro, la definizione di politiche interne per la comunicazione di incidenti TIC. I piani di crisi sono orientati alla gestione della comunicazione verso clienti, controparti, autorità e media nei casi di gravi incidenti o vulnerabilità significative. Le politiche, invece, riguardano l'informazione interna ai dipendenti, con una distinzione tra personale coinvolto direttamente nella gestione ICT e altri soggetti aziendali.

In termini sistemici, l'art. 14 e l'art. 45 convergono nell'obiettivo di rafforzare la resilienza collettiva, ma divergono per oggetto, destinatari e modalità di comunicazione. L'articolo 14 fonda la comunicazione su base obbligatoria e unilaterale, con logiche di *crisis management* e tutela del mercato; l'articolo 45 valorizza invece una logica volontaristica, basata sulla reciprocità e sulla creazione di comunità fidate, con l'obiettivo di arricchire il patrimonio informativo condiviso a fini preventivi.

Queste differenze si riflettono anche in ambito organizzativo: l'articolo 14 impone la nomina di almeno

3 Il Considerando (34) DORA stabilisce quanto segue: "*È opportuno incoraggiare le entità finanziarie a scambiarsi reciprocamente informazioni e analisi delle minacce informatiche e a sfruttare collettivamente, sul piano strategico, tattico e operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le proprie capacità di valutare e monitorare adeguatamente le minacce informatiche, difendersi dai loro effetti e rispondervi, partecipando a meccanismi di condivisione delle informazioni. È perciò necessario consentire l'emergere a livello dell'Unione di meccanismi volontari di condivisione delle informazioni i quali, se attuati in ambienti sicuri, aiuterebbero la comunità del settore finanziario a prevenire le minacce informatiche e a rispondervi collettivamente, contenendo rapidamente la diffusione dei rischi informatici e impedendo il potenziale contagio tramite i canali finanziari. Tali meccanismi dovrebbero essere conformi alle norme del diritto dell'Unione vigenti in materia di concorrenza di cui alla comunicazione della Commissione del 14 gennaio 2011 intitolata «Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale» nonché alle norme dell'Unione sulla protezione dei dati, in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (13). Essi dovrebbero operare sulla base del ricorso a una o più basi giuridiche stabilite all'articolo 6 di tale regolamento, ad esempio nel contesto del trattamento dei dati personali necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, ai sensi dell'articolo 6, paragrafo 1, lettera f), dello stesso regolamento, nonché nel contesto del trattamento dei dati personali necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento ai sensi dell'articolo 6, paragrafo 1, lettere c) ed e), rispettivamente, di tale regolamento.*".

un responsabile della comunicazione, quale punto di contatto interno per la gestione dell'informazione verso terzi in caso di incidente TIC. Tale profilo di responsabilità non è previsto dall'articolo 45, che invece demanda alle entità la definizione delle regole di partecipazione ai meccanismi volontari, incluso l'eventuale coinvolgimento delle autorità pubbliche e dei fornitori di servizi TIC.

Va sottolineato che la distinzione tra comunicazione obbligatoria e condivisione volontaria non comporta compartimenti stagni. Al contrario, entrambi gli articoli convergono nella richiesta di una *governance* strutturata di talché le due dimensioni devono essere considerate complementari all'interno del medesimo *framework* di *governance* ICT. È auspicabile che i piani di comunicazione delle crisi previsti dall'art. 14 integrino riferimenti operativi alla possibilità di attivare meccanismi di condivisione *ex* art. 45, specie nei casi in cui l'incidente generi indicatori di compromissione utili per la prevenzione collettiva.

Infine, va evidenziato come entrambi i regimi contribuiscano, in misura differente, a soddisfare il principio di "*security by transparency*" che attraversa il Regolamento DORA. La tempestiva informazione ai soggetti coinvolti da un incidente, così come la diffusione volontaria delle conoscenze utili alla prevenzione, si configurano come due modalità integrate di gestione del rischio ICT, fondate sul principio di collaborazione tra operatori e sulla fiducia come asset sistemico.

Nel loro insieme, in definitiva, appare ragionevole affermare che gli articoli 14 e 45 tracciano una traiettoria normativa che supera la visione proprietaria dell'informazione, promuovendo una nuova cultura della trasparenza nel settore finanziario, bilanciata da solidi presidi di sicurezza, governance e conformità regolamentare.

5. *Information sharing* e protezione dei dati personali: l'equilibrio necessario con il GDPR

Ebbene, è evidente come l'informazione condivisa tra le entità finanziarie può contenere – o essere suscettibile di contenere – dati personali, come indirizzi IP, e-mail aziendali, dati identificativi di clienti o dipendenti coinvolti in attacchi, o metadati generati in ambienti digitali. Ciò implica la necessità di una valutazione puntuale della liceità e proporzionalità del trattamento ai sensi del GDPR.

In primo luogo, le basi giuridiche previste dall'art. 6 del GDPR rappresentano il fondamento per qualsiasi trattamento connesso anche all'*information sharing*. Il Considerando (34) DORA e il Considerando (121)[4] della Direttiva (UE) 2022/2555 (cd. "NIS2") evidenziano tre possibili basi giuridiche rilevanti:

- l'obbligo legale (art. 6, par. 1, lett. c), nel caso di condivisioni richieste dalla normativa UE o nazionale;
- il compito di interesse pubblico (lett. e), quando lo scambio è funzionale alla sicurezza dei sistemi finanziari;
- il legittimo interesse del titolare del trattamento (lett. f), laddove supportato da un'adeguata va-

4 Secondo il Considerando (121) NIS2: "*Il trattamento dei dati personali, nella misura necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete da parte di soggetti essenziali e importanti, potrebbe essere considerato lecito in virtù del fatto che tale trattamento è conforme a un obbligo legale cui è soggetto il titolare del trattamento, conformemente ai requisiti di cui all'articolo 6, paragrafo 1, lettera c), e all'articolo 6, paragrafo 3, del regolamento (UE) 2016/679. Il trattamento dei dati personali potrebbe essere necessario anche per i legittimi interessi perseguiti dai soggetti essenziali e importanti, nonché dai fornitori di tecnologie e servizi di sicurezza che agiscono per conto di tali soggetti, a norma dell'articolo 6, paragrafo 1, lettera f), del regolamento (UE) 2016/679, anche qualora tale trattamento sia necessario per accordi di condivisione delle informazioni in materia di cibersicurezza o per la notifica volontaria di informazioni pertinenti a norma della presente direttiva. Le misure relative alla prevenzione, al rilevamento, all'individuazione, al contenimento e all'analisi degli incidenti e alla risposta agli stessi, le misure di sensibilizzazione in relazione a specifiche minacce informatiche, lo scambio di informazioni nel contesto della risoluzione e della divulgazione coordinata delle vulnerabilità, lo scambio volontario di informazioni su tali incidenti, sulle minacce informatiche e sulle vulnerabilità, sugli indicatori di compromissione, sulle tattiche, sulle tecniche e le procedure, sugli allarmi di cibersicurezza e sugli strumenti di configurazione potrebbero richiedere il trattamento di talune categorie di dati personali, quali indirizzi IP, localizzatori uniformi di risorse (URL), nomi di dominio, indirizzi di posta elettronica e, laddove rivelino dati personali, marcature temporali. Il trattamento dei dati personali da parte delle autorità competenti, dei punti di contatto unici e dei CSIRT potrebbe costituire un obbligo legale o essere considerato necessario per svolgere un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento ai sensi dell'articolo 6, paragrafo 1, lettera c) o e), e dell'articolo 6, paragrafo 3, del regolamento (UE) 2016/679, o per perseguire un interesse legittimo dei soggetti essenziali e importanti di cui all'articolo 6, paragrafo 1, lettera f), di tale regolamento. Inoltre, il diritto nazionale potrebbe stabilire norme che consentano alle autorità competenti, ai punti di contatto unici e ai CSIRT, nella misura necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete dei soggetti essenziali e importanti, di trattare categorie particolari di dati personali conformemente all'articolo 9 del regolamento (UE) 2016/679, in particolare prevedendo misure adeguate e specifiche per tutelare i diritti e gli interessi fondamentali delle persone fisiche, comprese limitazioni tecniche al riutilizzo di tali dati e l'uso di misure all'avanguardia in materia di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita*".

lutazione d'impatto (DPIA) e da misure tecniche e organizzative idonee.

La distinzione tra dati personali e dati non personali assume rilievo operativo. In linea con i principi di *data minimization* e *privacy by design* (art. 25 GDPR), le entità dovrebbero preferire l'utilizzo di tecniche di anonimizzazione o pseudonimizzazione, adottando protocolli di trasmissione cifrati, segmentazione delle informazioni e mascheramento degli identificativi.

Strumenti come la *privacy-enhancing technology* (PET), i *Data Loss Prevention* (DLP) *systems*, i protocolli STIX/TAXII e le tecniche di *hashing* possono contribuire ad abbattere il rischio di re-identificazione dei soggetti coinvolti, mantenendo l'utilità dell'informazione condivisa.

Il ruolo del DPO risulta centrale nell'implementazione di tali misure, poiché è tenuto a fornire pareri sulla compatibilità dei trattamenti con il GDPR, a supervisionare l'esecuzione dei DPIA (art. 35 GDPR) e a coordinarsi con il *Chief Information Security Officer* (CISO) per assicurare un approccio integrato.

La Corte di Giustizia dell'Unione Europea ha inoltre chiarito, in numerose pronunce[5], l'importanza della valutazione del rischio connesso alla trasmissione di dati, anche intra-UE, richiedendo misure supplementari di sicurezza in presenza di dati sensibili o flussi transfrontalieri.

Infine, la dottrina e le linee guida del WP29 (oggi EDPB) raccomandano di strutturare l'*information sharing* su basi modulari, con policy interne, registri delle attività, *accountability* trasversale, obblighi contrattuali per terze parti e verifiche periodiche di adeguatezza.

6. Intersezioni con la Direttiva NIS2: sinergie e criticità

La Direttiva NIS2 rafforza l'ecosistema normativo europeo in materia di *cybersicurezza*, incidendo su una vasta gamma di soggetti pubblici e privati, inclusi gli operatori essenziali del settore finanziario[6].

5 *Ex multis* cfr. C-311/18, Schrems II; C-210/16, Wirtschaftsakademie.

6 A tal proposito, appare opportuno sottolineare come il Regolamento DORA introduca un sistema armonizzato e vincolante di obblighi per i soggetti finanziari vigilati, configurandosi come *lex specialis* rispetto alla NIS 2. Invero, il considerando (28) della Direttiva NIS 2 chiarisce il rapporto tra la medesima e il Regolamento DORA, qualificando quest'ultimo come "*atto giuridico settoriale dell'Unione in relazione alla presente direttiva per quanto riguarda i soggetti del settore finanziario*". In tal senso, "*invece delle disposizioni stabilite nella presente direttiva dovrebbero applicarsi quelle del regolamento (UE) 2022/2554*" – con riferimento, tra l'altro, alle misure di gestione del rischio relativo alle tecnologie dell'informazione e della comunicazione (TIC), alla gestione e segnalazione degli incidenti gravi relativi alle TIC, ai test di resilienza operativa digitale, agli accordi di condivisione delle informazioni e ai rischi di terze parti – "*gli Stati membri non dovrebbero [...] applicare le disposizioni della presente direttiva riguardanti gli obblighi di gestione e segnalazione dei rischi di cibersicurezza e la vigilanza e l'esecuzione ai soggetti finanziari contemplati dal regolamento (UE) 2022/2554*". Al tempo stesso, il considerando evidenzia l'importanza di mantenere una solida relazione e uno scambio informativo tra le autorità competenti: a tal fine, il Regolamento DORA "*consente alle autorità europee di vigilanza (AEV) e alle autorità competenti [...] di partecipare alle attività del gruppo di cooperazione, di scambiare informazioni e cooperare con i punti di contatto unici, nonché con i CSIRT e le autorità competenti ai sensi della presente direttiva*".

7 Il Considerando (51) NIS2 prevede che: "*Gli Stati membri dovrebbero incoraggiare l'uso di ogni tecnologia innovativa, compresa l'intelligenza artificiale, il cui utilizzo potrebbe migliorare l'individuazione e la prevenzione degli attacchi informatici, consentendo di destinare in modo più efficace risorse per affrontare gli attacchi informatici. Gli Stati membri dovrebbero pertanto incoraggiare, nelle loro strategie nazionali per la cibersicurezza, le attività di ricerca e sviluppo volte a facilitare l'uso di tali tecnologie, in particolare quelle relative agli strumenti automatizzati o semiautomatizzati nella cibersicurezza, e, se del caso, la condivisione dei dati necessari per formare gli utenti di tali tecnologie e migliorarle. L'utilizzo di tutte le tecnologie innovative, compresa l'intelligenza artificiale, dovrebbe rispettare il diritto dell'Unione in materia di protezione dei dati, compresi i principi di protezione dei dati con riguardo all'accuratezza, alla minimizzazione dei dati, all'equità e alla trasparenza, nonché alla sicurezza dei dati, come la più recente crittografia. I requisiti di protezione dei dati fin dalla progettazione e predefiniti di cui al regolamento (UE) 2016/679 dovrebbero essere pienamente rispettati.*".

Il Considerando (121) della Direttiva riconosce espressamente che lo scambio di informazioni può comportare il trattamento di dati personali (es. IP, e-mail, URL), riaffermando l'obbligo di conformità con l'art. 6 GDPR.

Nel Considerando (51)[7], la Direttiva invita inoltre gli Stati membri a incentivare l'uso di tecnologie innovative – inclusa l'intelligenza artificiale – per potenziare le capacità di rilevamento e prevenzione delle minacce. Tuttavia, sottolinea la necessità di rispettare i principi di protezione dei dati fin dalla progettazione (*privacy by design*) e come impostazione predefinita (*by default*), nonché l'equità, la trasparenza e la minimizzazione del trattamento.

L'intersezione normativa tra NIS2 e DORA evidenzia il rischio di sovrapposizioni o conflitti tra autorità competenti, soprattutto per gli obblighi di notifica e cooperazione. È pertanto auspicabile che le autorità nazionali (es. ACN, Banca d'Italia, Garante Privacy) adottino approcci integrati e interoperabili, anche attraverso accordi di cooperazione o regolamenti congiunti.

vedi l'articolo online

Le sinergie si rilevano altresì nel potenziamento della risposta coordinata agli incidenti informatici e nella possibilità di condivisione di dati tra CERT finanziari e autorità nazionali, purché nel rispetto del principio di proporzionalità e dell'accountability.

Infine, il ricorso a sistemi AI e di analisi automatizzata delle minacce pone interrogativi su *bias*, *explainability* e rischi per i diritti fondamentali. La *compliance* ex GDPR e la futura interazione con l'AI Act rappresentano pertanto un altro snodo di convergenza e di attenzione per le entità finanziarie.

7. Prospettive operative: come implementare meccanismi di condivisione conformi al DORA

L'attuazione concreta dell'art. 45 DORA richiede una pianificazione multilivello. Le entità finanziarie devono costruire ecosistemi cooperativi stabili, affidabili e tecnicamente sicuri. Di seguito si propongono alcune direttrici operative:

a) Tecnologie abilitanti:

- piattaforme di *Threat Intelligence* (TIP), con funzionalità di analisi automatica, correlazione degli IoC e gestione dei flussi STIX/TAXII;
- strumenti di *Data Loss Prevention* (DLP) per controllare le informazioni in uscita e prevenire esfiltrazioni accidentali o dolose;
- sistemi di *logging*, *versioning* e *audit trail* per garantire la tracciabilità,

b) Strutture organizzative:

- nomina di un responsabile per l'*information sharing* (es. *Chief Threat Intelligence Officer*) e creazione di unità interfunzionali con CISO, DPO, legale e *risk manager*;
- *policy* e procedure approvate dal board, che definiscano perimetro informativo, ruoli, criteri di fiducia e meccanismi di escalation,

c) Accordi di riservatezza:

- NDA multilaterali o *contratti* quadro tra partecipanti, con clausole GDPR-*compliant*, obblighi di audit, tempi di *retention* e responsabilità reciproche,

d) Governance e partecipazione:

- partecipazione a ISAC settoriali, reti CERT, o meccanismi europei (es. FI-ISAC, ECSF) notificando l'adesione alle autorità competenti,

Un'attuazione efficace dell'art. 45 DORA, quindi, richiede non solo tecnologia e *compliance*, ma anche cultura organizzativa, cooperazione tra professionisti e presidio continuo della qualità informativa condivisa (nel pieno rispetto di tutti i presidi richiesti dalla normativa applicabile a tutela dei vari soggetti coinvolti).

8. Conclusioni: verso una cultura della resilienza collaborativa

L'art. 45 del Regolamento DORA codifica, per la prima volta in modo sistematico, una pratica di condivisione delle informazioni tra entità finanziarie in chiave regolamentata, volontaria ma strutturata, finalizzata a rafforzare la difesa collettiva contro le minacce informatiche. Si tratta di una rivoluzione culturale prima ancora che normativa, che impone agli operatori di abbandonare logiche di chiusura e competizione sulla sicurezza, in favore di un approccio cooperativo e fiduciario. Tuttavia, la piena efficacia del modello delineato dal DORA richiede un'attenta integrazione con il quadro normativo in materia di protezione dei dati personali, nonché l'attuazione di presidi tecnici, organizzativi e contrattuali idonei a garantire il rispetto dei principi di proporzionalità, accountability e responsabilità sociale d'impresa.

In tale direzione, la sfida per gli operatori finanziari è duplice: da un lato, aderire concretamente ai meccanismi di *sharing* previsti dall'art. 45, superando le tradizionali barriere reputazionali e giuridiche; dall'altro, assicurare un'effettiva integrazione tra le competenze del *Chief Information Security Officer* (CISO) e del *Data Protection Officer* (DPO), promuovendo una *governance* dei rischi digitali che sia realmente multidisciplinare e interfunzionale.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it