DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Cybersecurity e rapporti con le Autorità

Complessità operative ed impatti organizzativi

21 Luglio 2025

Savino Casamassima, Partner, Qubit Law Firm & Partners

DB non solo diritto bancario

Savino Casamassima, Partner, Qubit Law Firm & Partners

Savino Casamassima

Savino Casamassima è un Avvocato del Foro di Milano, Equity Partner di QubitLaw Firm & Partners. Assiste banche, intermediari finanziari e soggetti non vigilati, nella gestione di ogni aspetto relativo a revisione ed ottimizzazione dei processi interni, progetti di compliance, implementazione di nuove normative e strutturazione di modelli di governance, con particolare riferimento alle funzioni di controllo ed alla definizione di assetti organizzativi integrati. Ha ricoperto funzioni apicali in ambito sia legale che compliance presso banche internazionali e società operanti nel mondo dei servizi bancari e fintech. È stato altresì membro di Consigli di Amministrazione ed Organismi di Vigilanza 231 presso banche ed intermediari finanziari internazionali.

QUBIT LAW FIRM & PARTNERS

1. Premessa

A partire dal 2016 con l'introduzione della regolamentazione GDPR, il legislatore europeo ha progressivamente rafforzato il quadro normativo in materia di cybersicurezza e protezione dei dati personali, introducendo obblighi di segnalazione sempre più stringenti a carico di imprese pubbliche e private. Le principali normative di riferimento — **GDPR**, **NIS2** e **DORA** — impongono requisiti di notifica per incidenti significativi, violazioni di dati personali (*data breach*) e disservizi con impatti operativi rilevanti. Tuttavia, l'eterogeneità di tali obblighi e la mancata armonizzazione dei processi comportano spesso una **sovrapposizione di attività**, che rischia di complicare i rapporti con le Autorità competenti ed aumentare il carico amministrativo per le imprese.

Questo articolo intende analizzare il tema della **sovrapposizione tra i processi di segnalazione**, **le implicazioni organizzative** e le possibili soluzioni per una gestione efficiente e conforme agli obblighi normativi.

2. I rapporti con le Autorità: sovrapposizione dei processi sulle segnalazioni degli incidenti significativi e dei *data breach*.

2.1. *Il quadro normativo europeo: GDPR, NIS2 e DORA*

Il **GDPR** (**Regolamento Generale sulla Protezione dei Dati del 2016**) ha introdotto nel 2016 l'obbligo di notificare al **Garante per la Protezione dei Dati personali**, quale autorità competente, l'incidente di sicurezza che comporti la violazione dei dati personali (*data breach*) entro **72 ore** dalla scoperta dell'incidente, ai sensi dell'articolo 33, e ciò riguarda **tutti i titolari e responsabili del trattamento** di dati personali, indipendentemente dal settore di appartenenza. In caso di rischio elevato per i diritti e le libertà degli interessati, è inoltre necessario informare anche gli **interessati** coinvolti.

Successivamente è intervenuta nel 2022 la **Direttiva UE NIS2 (2022/2555) sulla sicurezza delle reti e dei sistemi informativi**, che ha sostituito la precedente NIS (Direttiva UE 2016/1148) ed ampliato il perimetro dei soggetti obbligati includendo **enti essenziali e importanti** operanti in numerosi settori critici (energia, trasporti, finanza, sanità, ICT, ecc.).

In particolare, ai sensi dell'art. 23, le entità soggette devono notificare **qualsiasi incidente con impatto significativo sulla fornitura dei servizi** entro termini molto brevi, ovvero **24 ore** per una notifica preliminare, **72 ore** per una notifica completa e **1 mese** per una relazione finale e, a tal fine, l'autorità competente in Italia è l'**ACN** (Agenzia per la Cybersicurezza Nazionale).

Da ultimo **DORA, ovvero il *Digital Operational Resilience Act* (Regolamento UE 2022/2554)** è rivolto specificamente al settore finanziario e impone l'obbligo di notifica degli **incidenti ICT significativi** alle Autorità di Vigilanza preposte. In particolare, il **Regolamento Delegato 2025/301, in attuazione del-**

vedi l'articolo online

la normativa DORA, prevede che gli incidenti gravi debbano essere notificati per la relazione iniziale quanto prima, ma in ogni caso entro quattro ore dalla classificazione dell'incidente connesso alle TIC come grave ed entro 24 ore dal momento in cui l'entità finanziaria è venuta a conoscenza dell'incidente connesso alle TIC; per la relazione intermedia al più tardi entro 72 ore dalla trasmissione della notifica iniziale, anche se lo stato o il trattamento dell'incidente non sono cambiati, mentre la relazione finale deve essere trasmessa entro un mese dall'ultima relazione intermedia aggiornata. DORA, inoltre, introduce sin da subito criteri stringenti di **classificazione dell'incidente**, basati su impatto operativo, numero di clienti colpiti, perdita economica, e impatto reputazionale. In questo caso, l'Autorità preposta nell'implementazione italiana è la **Banca d'Italia**.

2.2. *La sovrapposizione dei processi di notifica: il problema*

La conseguenza della stratificazione normativa sopra evidenziata, quindi, è che un singolo incidente può attivare obblighi di notifica diversi verso Autorità differenti. Si consideri ad esempio un attacco ransomware che:

- compromette i dati personali → GDPR
- interrompe l'erogazione di un servizio critico → NIS2
- ha impatti operativi rilevanti su una banca → DORA

In questo caso, l'organizzazione deve notificare:

- il Garante Privacy entro 72 ore (GDPR)
- l'ACN entro 24/72 ore (NIS2)
- la Banca d'Italia entro il termine di 4/24 ore (DORA)

Inoltre, ognuna delle normative menzionate adotta **criteri distinti per la valutazione della significatività** dell'incidente, poiché il Regolamento GDPR si focalizza sul rischio per i diritti degli interessati, la Direttiva NIS2 sull'impatto sulla continuità dei servizi ed il Regolamento DORA sull'impatto operativo e reputazionale nel settore finanziario.

Queste differenze creano **ambiguità e complessità operative**, rendendo difficile per le imprese stabilire quando e come effettuare le notifiche, considerando peraltro che ogni normativa prevede **modelli e canali diversi** per la trasmissione delle segnalazioni:

- il GDPR richiede la compilazione di specifici moduli per il Garante
- l'ACN ha introdotto il **portale CSIRT** per la notifica degli incidenti
- il DORA impone modelli standardizzati secondo linee guida EBA/EIOPA/ESMA

Questo implica **duplicazione del lavoro** e necessità di mantenere **piattaforme e procedure multiple**, con rischi di errore ed incongruenze.

Peraltro, **la differenza non riguarda solo i destinatari, le tempistiche e le modalità, ma gli stessi contenuti delle notifiche che non sono perfettamente sovrapponibili** in quanto:

Per la normativa GDPR i contenuti principali della notifica al Garante ai sensi degli artt. 33 e 34 sono:

- Natura della violazione (riservatezza, integrità, disponibilità);
- Categorie e numero approssimativo di interessati e di record coinvolti;
- Nome e contatti del DPO o altro referente;
- Probabili conseguenze della violazione;
- Misure adottate o proposte per porre rimedio e mitigare gli effetti.

Per la Direttiva NIS2 (Direttiva UE 2022/2555) i contenuti principali della notifica ad ACN sono:

- Descrizione iniziale dell'incidente, con aggiornamenti successivi (entro 24 ore notifica preliminare, entro 72 ore notifica completa);
- Impatti significativi sul servizio (es. interruzione, danni economici, effetti transfrontalieri);
- Indicatori di compromissione, cause e vettori dell'attacco;
- Misure correttive adottate o pianificate.

Ai sensi del Regolamento DORA (Reg. UE 2022/2554) i contenuti principali della notifica a Banca d'Italia sono:

- Descrizione dell'incidente significativo e impatti sui servizi critici;
- Sistemi, processi o funzioni impattate;

- Classificazione e gravità dell'incidente (conformemente ai criteri normativi);
- Impatto sulla disponibilità, integrità e confidenzialità;
- Dettagli su fornitori terzi coinvolti (se rilevanti);
- Misure adottate per contenere e ripristinare le attività.

A corollario di quanto sopra, poi, rimane la difficoltà oggettiva di una **interlocuzione sulla medesima criticità con diverse Autorità sulla base di normative differenti che colgono "interessi", seppur convergenti, diversi**; tale complessità potrà essere mitigata dagli Accordi di Protocollo tra le Autorità che progressivamente verranno implementati, sia a livello nazionale che europeo, i quali tuttavia non potranno cancellare le differenze sostanziali e le diverse "tutele" in gioco.

3. Gli impatti organizzativi delle normative GDPR, NIS2 e DORA: nuove competenze e processi integrati

La coesistenza di più regimi normativi impone certamente processi armonizzati, che consentano di effettuare valutazioni trasversali ed univoche e questo obbiettivo può essere raggiunto, ad esempio, attraverso una gestione integrata delle notifiche, in cui il primo passo è realizzare una **mappatura completa** delle normative applicabili, dei soggetti coinvolti e delle scadenze previste. Ogni incidente deve essere valutato in base ad una **matrice multidimensionale** che consideri; (i) natura dell'impatto (dati, servizi, finanza); (ii) rilevanza geografica e settoriale e (iii) tipologia dei dati e delle vittime coinvolte.

È utile, inoltre, implementare un **processo unificato di gestione degli incidenti**, che preveda un unico punto o team di coordinamento (es. Incident Response Team), fasi predefinite (identificazione, analisi, classificazione, notifica, post-mortem) ed automatismi per la compilazione dei diversi modelli di segnalazione. L'allineamento dei processi, tuttavia, deve necessariamente essere accompagnata da nuove competenze trasversali ed integrate **delle funzioni di compliance e cybersecurity**, nonché da una collaborazione continua tra le stesse.

3.1. ***Funzioni organizzative rilevanti***

Il modello organizzativo più adatto, probabilmente, **può essere quello regolamentare**, tipico delle entità soggette alla regolamentazione DORA, il quale potrà essere "esportato" al di fuori del mondo delle entità finanziarie, al fine di creare un modello di organizzazione affidabile e solido relativamente ai controlli compliance e cybersecurity.

In particolare, le funzioni specifiche da inserire o, se già presenti, rafforzare, sempre tenendo conto di un'adeguata applicazione del principio di proporzionalità sono:

- **Data Governance**

La prima funzione da istituire, se non già esistente, è quella di **Data Governance** (o "governo dei dati") che si occupa di **definire, gestire e controllare** il modo in cui i dati vengono raccolti, archiviati, utilizzati e protetti all'interno di un'organizzazione. Il suo obiettivo principale è garantire che i dati siano **accurati, accessibili, consistenti, sicuri e utilizzati in modo conforme** alle normative e alle policy aziendali. Le principali attività della funzione di Data Governance includono: definizione delle politiche e degli standard sui dati, gestione della qualità dei dati, classificazione e catalogazione dei dati, data lineage e tracciabilità, gestione degli accessi e della sicurezza dei dati, conformità normativa e audit di I livello (soprattutto relativamente a GDPR, NIS2, DORA, ecc.), nonché supporto alla strategia aziendale ed all'analisi dei dati.

La Data Governance, così concepita, diventa **una funzione strategica**, non solo tecnica, che si pone tra **IT, compliance, risk management e business**, ed è fondamentale in un contesto dove i dati sono considerati un asset critico, specialmente per settori regolamentati come finanza, sanità, energia e pubblica amministrazione.

- **CISO (Chief Information Security Officer)**

La seconda figura, introdotta da DORA, ma che può essere altresì "esportata" al di fuori del mondo regolamentare, è quella del CISO (Chief Information Security Officer) quale dirigente responsabile della **sicurezza delle informazioni** all'interno di un'organizzazione. La sua funzione principale è **proteggere i dati, i sistemi e le infrastrutture IT** da minacce interne ed esterne, garantendo la **conformità normativa**, la **continuità operativa** e la **resilienza informatica**. I suoi obbiettivi principali sono: la definizione della strategia di cybersecurity, la gestione del rischio informatico, la supervisione della sicurezza operativa, l'Incident response e gestione delle crisi, la assurance della conformità normativa su sicurezza e privacy (es. GDPR, NIS2, DORA, ISO/IEC 27001), anche attraverso la predisposizione di controlli ed il supporto ad audit interni ed esterni, l'implementazione dell'awareness e della formazione e introduzione del sistema di governance e di reporting al **CEO, al CDA o al Comitato Rischi** sull'efficacia delle misure di sicurezza, nonché la partecipazione alla definizione della **Data Governance**, della **Business Continuity** e della **resilienza operativa**.

Il CISO, quindi, è una **figura di controllo (II livello) chiave nella resilienza digitale dell'organizzazione**. In un contesto normativo europeo sempre più stringente (DORA, NIS2, GDPR), il CISO deve **coniugare competenze tecniche, gestionali e legali**, ed è spesso coinvolto nei rapporti con le **autorità di vigilanza**, in particolare in caso di **segnalazioni di incidenti significativi**.

- **DPO (Data Protection Officer)**

È evidente come la figura del DPO, seppure non nuova poiché istituita dal Regolamento GDPR nel 2016,

vedi l'articolo online

in questo contesto vada sicuramente armonizzata al nuovo contesto normativo. Il **DPO** (Data Protection Officer), o **Responsabile della Protezione dei Dati**, infatti è una figura già prevista dal **GDPR** ed il suo ruolo è garantire che l'organizzazione **tratti i dati personali in modo conforme** al GDPR e alle normative nazionali in materia di privacy.

Le sue principali funzioni sono la sorveglianza sulla conformità in materia di protezione dei dati, la consulenza al titolare e ai responsabili del trattamento, l'attività di coordinamento nei rapporti con **il Garante per la Protezione dei Dati Personali**, anche in caso di attività ispettive o di verifica e in caso di **data breach**, la gestione delle richieste degli interessati, la formazione e sensibilizzazione dei destinatari della normativa ed il monitoraggio delle valutazioni d'impatto (DPIA). È una funzione che deve avere i requisiti dell'indipendenza (organizzativa), competenza ed assenza di conflitto di interessi (sulle attività svolte).

Il DPO è il **garante interno della privacy**: supervisiona (III livello di controllo), consiglia, forma e funge da collegamento tra l'organizzazione, gli interessati ed il Garante. È una figura **strategica e indipendente**, fondamentale per assicurare il rispetto della normativa e per **ridurre il rischio di sanzioni e danni reputazionali**.

Le figure di cui sopra, quindi, **vanno ad aggiungersi a quelle tradizionali della Compliance, Risk Management, Legal ed IT**, anch'esse da integrare pienamente in un modello organizzativo virtuoso nella gestione della sicurezza dei dati e della sicurezza informatica, in cui sono chiamate a giocare un ruolo "di squadra" e, quindi, ad avere competenze e skill non solo adeguati, ma anche trasversali.

3.2. *Modello organizzativo e Comitati*

Il modello organizzativo ideale, quindi, in una struttura di media/alta complessità, include la figura del **Data Governance Manager** quale **funzione senior apicale strategica a supporto del *business***, in grado di interagire con il **CISO, quale funzione di controllo di II livello, ed il DPO, quale funzione di controllo di III livello**.

In questo contesto, **le funzioni di Compliance ed il Risk Management possono costituire un ulteriore presidio**, nei rispettivi ruoli, con un **modello organizzativo integrato, anche attraverso l'istituzione di idonei Comitati**, che consenta una supervisione ampia, allo stesso tempo priva di rischi e focalizzata sul supporto alle aree commerciali e di *business*. **La funzione Legal**, da ultimo, oltre a fornire **idoneo supporto tecnico**, soprattutto se coinvolta negli affari societari, potrà svolgere un **ruolo residuale attivo nelle relazioni istituzionali** stabilendo canali **di comunicazione preventiva** con le Autorità di riferimento finalizzati a facilitare la gestione degli obblighi attraverso la partecipazione a tavoli di lavoro istituzionali, nonché eventuali richieste di chiarimenti su casi o interpretazioni normative dubbie.

Le organizzazioni, inoltre, devono sviluppare **processi interni rapidi ed efficaci di *detection*, analisi e notifica**, spesso entro poche ore e questo richiede processi che armonizzano le implicazioni normative sopra evidenziate.

Il personale coinvolto nella gestione degli incidenti, inoltre, deve essere **formato su più normative**, con una competenza trasversale in ambito GDPR, NIS2 e DORA, con la conseguenza che non solo risultano assolutamente necessari corsi di formazione specifici per il personale tecnico e legale, simulazioni periodiche e procedure interne costantemente aggiornate, ma si rende quanto mai necessario da un punto di vista organizzativo l'**utilizzo di piattaforme integrate** di rilevamento automatico degli incidenti ed attivazione automatica dei flussi di notifica verso le Autorità.

3.3. *Prospettive di armonizzazione normativa*

La Commissione Europea ha avviato una riflessione su una **maggiore armonizzazione dei processi di segnalazione**, anche in ottica di interoperabilità tra le normative, con alcune proposte che includono la creazione di **moduli di notifica unificati** validi per più regolamenti, l'introduzione di **sportelli unici** per la ricezione centralizzata delle segnalazioni ed il rafforzamento del ruolo dell'**ENISA** nel coordinamento tra le Autorità.

In questo contesto, le Autorità Nazionali italiane si sono già attivate per la creazione di protocolli operativi comuni, Linee guida integrate per la gestione degli incidenti e Sistemi informatici interconnessi.

4. Conclusioni

In **meno di 10 anni**, dal GDPR nel 2016 ad oggi, il mondo della gestione dei dati, con particolare riferimento ai profili della sicurezza, è cresciuto in modo esponenziale per complessità ed ampiezza, in una dimensione globale e collettiva da cui ormai non si tornerà più indietro e che, con le implicazioni della nuova normativa sull'Artificial Intelligence non potrà che amplificarsi ulteriormente.

In questo senso, quindi, rappresenta un'evidenza di grande maturità e consapevolezza **il principio normativo ormai sdoganato di tutela collettiva e condivisione delle informazioni, che caratterizza soprattutto NIS2 e GDPR**: sulla cybersecurity nessuno si tutela da solo.

In modo speculare, tale crescente complessità comporta per le imprese un onere significativo in termini di **tempestività, accuratezza e coordinamento** nella gestione degli incidenti. La **sovrapposizione dei processi di notifica** tra GDPR, NIS2 e DORA rappresenta una sfida concreta, che richiede si da subito un approccio integrato e strategico.

Solo attraverso una **gestion<<<<<<<e strutturata, interdisciplinare e proattiva** sarà possibile trasformare gli obblighi normativi in un'opportunità per rafforzare la resilienza digitale e consolidare la fiducia nei confronti delle Autorità e degli stakeholder.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it