DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

NIS2 e DORA: tra specificità e profili di coordinamento

7 Gennaio 2026

Savino Casamassima, Partner, Qubit Law Firm & Partners

Savino Casamassima, Partner, Qubit Law Firm & Partners

Savino Casamassima

Savino Casamassima è un Avvocato del Foro di Milano. Ha una significativa esperienza presso studi legali italiani ed internazionali a Milano e Londra ed ha ricoperto funzioni apicali in ambito sia legale che compliance presso banche internazionali e società operanti nel mondo dei servizi bancari e fintech. Già membro di Consigli di Amministrazione ed Organismi di Vigilanza 231 presso banche ed intermediari finanziari internazionali.

1. Premessa: il necessario coordinamento normativo e regolamentare

L'evoluzione del quadro normativo europeo in materia di sicurezza informatica e resilienza digitale riflette la crescente centralità delle tecnologie dell'informazione nei processi economici e, in particolare, nel funzionamento del sistema finanziario. L'interconnessione tra infrastrutture digitali, mercati finanziari e servizi essenziali ha reso evidente come gli incidenti informatici non costituiscano più eventi isolati, ma potenziali fattori di rischio sistemico, in grado di incidere sulla stabilità finanziaria, sulla fiducia degli operatori e sulla tutela degli utenti finali.

In questo scenario si inseriscono il Regolamento (UE) 2022/2554, noto come Digital Operational Resilience Act (DORA), e la Direttiva (UE) 2022/2555 (NIS2), che, in un'ottica complementare, definiscono il quadro europeo di riferimento per la resilienza operativa digitale del settore finanziario. Il loro **coordinamento è decisivo per le entità finanziarie, chiamate a confrontarsi con un livello di regolazione senza precedenti in materia di governance ICT, gestione del rischio e responsabilità degli organi aziendali**.

2. DORA come disciplina settoriale di riferimento per il settore finanziario

Il Regolamento (UE) 2022/2554, noto come Digital Operational Resilience Act (DORA), si inserisce nel processo di progressiva razionalizzazione della disciplina europea in materia di rischio ICT, con l'obiettivo di superare la frammentazione normativa che ha a lungo caratterizzato il settore finanziario. Prima della sua adozione, gli intermediari erano chiamati a conformarsi a un insieme eterogeneo di disposizioni di matrice nazionale, linee guida delle autorità di vigilanza e standard di *soft law*, spesso non pienamente coordinati tra loro, scenario particolarmente critico per le entità operanti su base transfrontaliera e penalizzante per la realizzazione del mercato unico dei servizi finanziari digitali.

In questo contesto, DORA introduce un quadro regolamentare unitario e direttamente applicabile, assumendo espressamente la funzione di disciplina settoriale speciale in materia di resilienza operativa digitale. Il legislatore europeo ha collocato il Regolamento all'interno dell'ecosistema della cybersecurity come *lex specialis* rispetto alla normativa orizzontale, in particolare alla Direttiva (UE) 2022/2555 (NIS2), riconoscendo che il settore finanziario, per la sua rilevanza sistemica e per l'elevato grado di digitalizzazione dei processi, richiede regole più puntuali e stringenti rispetto a quelle previste per la

vedi l'articolo online

generalità dei settori economici.

Il rapporto tra DORA e NIS2 si fonda su un criterio di specialità funzionale: mentre la Direttiva NIS2 definisce un quadro orizzontale volto ad assicurare un livello elevato e uniforme di cybersicurezza nell'Unione, DORA disciplina in modo esaustivo e settoriale le misure di gestione del rischio ICT, la gestione e la segnalazione degli incidenti, i test di resilienza operativa digitale e il controllo dei rischi derivanti da terze parti ICT per le entità finanziarie. Ne deriva che, **per i soggetti rientranti nell'ambito di applicazione del Regolamento, le disposizioni di DORA prevalgono su quelle della NIS2 per i profili coincidenti, evitando duplicazioni normative e sovrapposizioni applicative**.

Uno degli elementi qualificanti del Regolamento è rappresentato dal rafforzamento della governance del rischio ICT: la resilienza operativa digitale viene ricondotta nell'alveo delle responsabilità strategiche degli organi di amministrazione e controllo, chiamati a svolgere un ruolo attivo e consapevole nella definizione, approvazione e supervisione dei presidi di sicurezza tecnologica. La gestione del rischio ICT non è più confinata a una dimensione tecnica o operativa, ma diviene parte integrante dei processi decisionali dell'ente, in coerenza con l'impostazione della NIS2, che parimenti enfatizza il ruolo degli organi apicali secondo una logica orizzontale e multisettoriale.

Accanto al profilo organizzativo, DORA introduce un sistema armonizzato di gestione e segnalazione degli incidenti ICT, fondato su criteri uniformi di classificazione e su tempistiche di notifica comuni a livello unionale. Anche in questo ambito, **il coordinamento con la NIS2 è espressamente perseguito: il Regolamento sostituisce, per le entità finanziarie, gli obblighi di notifica previsti dalla disciplina orizzontale, ma mantiene un canale di raccordo informativo con l'ecosistema NIS, così da garantire una visione complessiva del panorama delle minacce informatiche nell'Unione**.

Particolare attenzione è, infine, riservata al rischio derivante dal ricorso a fornitori terzi di servizi ICT. La crescente dipendenza delle entità finanziarie da soggetti esterni, soprattutto nel contesto dei servizi cloud, è affrontata attraverso un insieme articolato di obblighi di due diligence, requisiti contrattuali rafforzati e meccanismi di supervisione a livello europeo; anche qui DORA si coordina con la NIS2, configurando un modello di regolazione complementare in cui alla vigilanza settoriale sulle entità finanziarie si affianca il quadro orizzontale di cybersicurezza applicabile ai fornitori ICT, con l'obiettivo di presidiare l'intera catena del valore digitale.

3. Il ruolo residuale della Direttiva NIS2 per le entità finanziarie

L'adozione del Regolamento DORA ha profondamente ridefinito il rapporto tra la disciplina settoriale della resilienza operativa digitale ed il quadro orizzontale europeo in materia di cybersicurezza delineato dalla Direttiva (UE) 2022/2555 (NIS2). Ciò nondimeno, **la NIS2 non è integralmente espunta dall'orizzonte regolamentare delle entità finanziarie, ma continua a trovare applicazione in una serie di profili residuali**, prevalentemente esterni al perimetro strettamente prudenziale e micro-settoriale presidiato da DORA, funzionali a preservare la coerenza dell'ecosistema europeo della cybersicurezza ed a garantire un livello uniforme di protezione a livello sistemico ed intersettoriale.

Un primo ambito di rilevanza residuale riguarda il coordinamento istituzionale e informativo a livello nazionale ed europeo. Le entità finanziarie, pur soggette alla vigilanza settoriale delle autorità competenti ai sensi di DORA, restano inserite nell'ecosistema di cooperazione previsto dalla NIS2, che comprende i CSIRT nazionali, il Gruppo di cooperazione e i meccanismi di gestione delle crisi informatiche su vasta scala, consentendo alle autorità di cybersicurezza di disporre di una visione complessiva delle minacce che interessano settori diversi e di coordinare le risposte in presenza di incidenti che eccedono la dimensione settoriale e assumono rilievo sistemico o transfrontaliero.

Un secondo profilo concerne la gestione delle crisi cibernetiche su larga scala. DORA disciplina in modo puntuale la gestione e la notifica degli incidenti ICT rilevanti per le singole entità finanziarie e per la stabilità del sistema finanziario, mentre la NIS2 conserva un ruolo centrale nella regolazione delle crisi che coinvolgono più settori critici o più Stati membri, tramite i meccanismi di coordinamento della Direttiva, in particolare le strutture di crisi nazionali e l'EU-CyCLONe, che continuano ad applicarsi anche agli incidenti che interessano il settore finanziario, raccordando resilienza settoriale e sicurezza collettiva dell'Unione.

Ulteriore ambito di applicazione residuale è rappresentato dal perimetro soggettivo non integralmente coincidente con quello di DORA. Nei gruppi complessi che comprendono entità finanziarie e soggetti non finanziari, questi ultimi restano pienamente soggetti alla disciplina NIS2, con la conseguenza che le capogruppo devono coordinare modelli di governance e di gestione del rischio diffe-

renziati ma coerenti; analogamente, **la NIS2 continua ad applicarsi direttamente ai fornitori ICT che non siano qualificati come fornitori terzi critici ai sensi di DORA, ma che rientrano comunque tra i soggetti essenziali o importanti della Direttiva**.

La NIS2 mantiene inoltre una rilevanza indiretta sul piano delle strategie nazionali di cybersicurezza e delle politiche pubbliche di prevenzione, alle quali le entità finanziarie restano funzionalmente collegate. Pur non essendo direttamente soggette agli obblighi operativi della Direttiva per i profili coperti da DORA, esse continuano a inserirsi nel quadro strategico e sistemico delineato a livello statale ed europeo, contribuendo, anche mediante lo scambio informativo, alla resilienza complessiva delle infrastrutture digitali.

In questa prospettiva, **il rapporto tra DORA e NIS2 non si configura come un'alternativa tra discipline concorrenti, ma come un modello di specialità integrata**, nel quale la normativa settoriale finanziaria assorbe gli obblighi operativi più stringenti, mentre la Direttiva orizzontale conserva un ruolo di sfondo essenziale per il coordinamento intersettoriale e la gestione delle minacce cibernetiche di dimensione sistemica.

4. La trasversalità del GDPR nel contesto DORA–NIS2

Il Regolamento (UE) 2016/679 (GDPR) si colloca temporalmente e sistematicamente in una fase antecedente rispetto all'adozione di DORA e della Direttiva NIS2, ma continua a rappresentare un pilastro imprescindibile del quadro europeo della sicurezza digitale. **Pur non essendo stato concepito originariamente come normativa di cybersicurezza in senso stretto, il GDPR ha introdotto per la prima volta nell'ordinamento dell'Unione un modello giuridico organico di gestione del rischio informatico**, fondato sulla protezione dei dati personali come valore fondamentale e sulla responsabilizzazione degli attori coinvolti nei trattamenti.

In tale prospettiva, **il GDPR svolge una funzione trasversale che attraversa e integra tanto la disciplina settoriale di DORA quanto l'impianto orizzontale della NIS2**. La sicurezza del trattamento dei dati personali, declinata attraverso i principi di integrità, riservatezza e disponibilità, costituisce infatti un punto di convergenza strutturale tra le diverse normative, ponendosi come base comune su cui si innestano gli obblighi più specifici in materia di resilienza operativa digitale e di gestione degli incidenti informatici.

L'importanza del GDPR in ambito cybersecurity **emerge in modo particolare nella disciplina delle misure di sicurezza e nella gestione degli incidenti**. L'obbligo di adottare misure tecniche e organizzative adeguate al rischio e il meccanismo di notifica delle violazioni dei dati personali hanno anticipato – e in parte ispirato – l'impostazione risk-based successivamente ripresa e sviluppata sia dalla NIS2 sia da DORA, estendendo progressivamente la logica della gestione del rischio dal perimetro della protezione dei dati personali a quello, più ampio, della resilienza digitale dei sistemi e delle infrastrutture critiche.

Nel contesto delle entità finanziarie, questa trasversalità assume una valenza ancora più marcata. Gli incidenti ICT disciplinati da DORA presentano frequentemente un impatto anche sul trattamento dei dati personali, con la conseguenza che le organizzazioni devono valutare in modo coordinato profili di resilienza operativa, continuità dei servizi e tutela dei diritti e delle libertà degli interessati, evitando una gestione frammentata e settoriale degli eventi di sicurezza.

Sotto il profilo organizzativo, il GDPR continua a svolgere una funzione di integrazione essenziale. **Le figure e i processi introdotti dalla disciplina in materia di protezione dei dati personali** – in particolare il Data Protection Officer, le valutazioni d'impatto e i registri delle attività di trattamento – **rappresentano oggi elementi chiave dei modelli di governance della sicurezza informatica**, creando un linguaggio comune e un patrimonio condiviso di competenze che facilita il dialogo tra funzioni giuridiche, tecniche e di business, in linea con le esigenze di integrazione richieste da DORA e NIS2.

Infine, il GDPR mantiene un ruolo centrale anche sul piano delle competenze e della cultura organizzativa. Il principio di accountability, che impone non solo il rispetto formale degli obblighi ma anche la capacità di dimostrarne l'effettiva attuazione, permea ormai l'intero ecosistema normativo europeo della cybersecurity, **sicché il GDPR non rappresenta una disciplina meramente ancillare rispetto a DORA e NIS2, ma il fondamento trasversale su cui si innestano e si coordinano le più recenti normative in materia di resilienza operativa digitale e sicurezza delle reti e dei sistemi informativi**.

5. La prospettiva della Digital Omnibus e il coordinamento normativo

Nel quadro di progressiva stratificazione del diritto digitale dell'Unione europea, la proposta di Regolamento comunemente indicata come Digital Omnibus si colloca come intervento di razionalizzazione sistemica, volto a semplificare, coordinare e rendere maggiormente coerente l'insieme delle normative che compongono il cosiddetto *digital acquis*. Pur trattandosi, allo stato, di una disciplina ancora in fase di elaborazione e negoziazione, la sua rilevanza emerge con particolare chiarezza rispetto all'interazione tra GDPR, NIS2 e DORA, ambiti nei quali il rischio di sovrapposizioni e duplicazioni applicative si è manifestato in modo particolarmente evidente.

La logica sottesa alla Digital Omnibus non è quella di introdurre nuovi obblighi sostanziali, bensì di intervenire in chiave correttiva e di coordinamento, preservando gli obiettivi di tutela perseguiti dalle singole normative settoriali e orizzontali, ma riducendo la complessità derivante dalla loro applicazione congiunta. In tale prospettiva, la Commissione europea ha individuato nella frammentazione degli obblighi di compliance – in particolare in materia di gestione del rischio, sicurezza informatica e notificazione degli incidenti – uno dei principali fattori di inefficienza per operatori economici e autorità pubbliche.

Con specifico riferimento al rapporto tra NIS2 e DORA, la Digital Omnibus mira a rafforzare il principio di specialità settoriale già delineato dal legislatore unionale, chiarendo ulteriormente che le entità finanziarie soggette a DORA devono poter fare affidamento su un quadro unitario di obblighi in materia di resilienza operativa digitale. In questa direzione si colloca, in particolare, la **proposta di razionalizzazione dei meccanismi di segnalazione degli incidenti informatici**, volta a ricondurre sotto un'unica architettura di reporting gli obblighi previsti dalle diverse normative, evitando duplicazioni e incoerenze procedurali, con un impatto diretto sulla riduzione dell'onere per le entità finanziarie.

La funzione di coordinamento della Digital Omnibus si manifesta in modo significativo anche rispetto al GDPR. La proposta riconosce esplicitamente il ruolo della disciplina in materia di protezione dei dati personali come fondamento trasversale dell'intero ecosistema digitale europeo, riaffermandone la centralità e intervenendo per chiarire taluni profili applicativi che incidono direttamente sulla cybersecurity, quali la nozione di violazione dei dati personali, gli obblighi informativi e i rapporti tra sicurezza del trattamento e altri obblighi settoriali. In questo modo, **il GDPR viene confermato – anche nella prospettiva della futura riforma – come asse portante di integrazione normativa, capace di connettere la logica della resilienza operativa digitale con la tutela dei diritti fondamentali**.

Sul piano sistemico, la Digital Omnibus si propone dunque come strumento di raccordo tra normative che perseguono finalità convergenti ma operano su piani differenti: la stabilità e continuità dei servizi finanziari nel caso di DORA, la sicurezza delle reti e dei sistemi informativi nel caso della NIS2, la protezione dei dati personali e la responsabilizzazione degli operatori nel caso del GDPR. L'obiettivo dichiarato è favorire un'applicazione coordinata e coerente di tali discipline, riducendo l'onere amministrativo senza compromettere gli standard di sicurezza e di tutela raggiunti, pur nel rispetto del carattere ancora propositivo e non definitivo dell'intervento regolamentare.

In questa prospettiva, la Digital Omnibus contribuisce a delineare, se e nella misura in cui verrà adottata nella sua formulazione finale, un modello di regolazione integrata in cui il coordinamento normativo si accompagna a una progressiva integrazione organizzativa e di competenze all'interno delle imprese e delle autorità di controllo. **Pur senza incidere direttamente sulle architetture di governance settoriale, la proposta rafforza l'idea di un diritto digitale europeo sempre più orientato alla coerenza sistemica, nel quale GDPR, NIS2 e DORA non operano come compartimenti stagni, ma come elementi di un quadro regolatorio unitario e interconnesso**.

6. Il Perimetro di sicurezza cibernetica nazionale nel contesto europeo: integrazione e coordinamento con NIS2, DORA e GDPR

Il Perimetro di sicurezza cibernetica nazionale, introdotto dal decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla legge 18 novembre 2019, n. 133, rappresenta uno degli **strumenti centrali attraverso cui l'ordinamento italiano ha inteso rafforzare la tutela degli interessi strategici dello Stato nel dominio digitale**. La disciplina si fonda su un approccio selettivo e funzionale, volto a individuare soggetti pubblici e privati che svolgono funzioni essenziali o servizi di rilevanza strategica, la cui compromissione può incidere sulla sicurezza nazionale, sull'ordine pubblico o sulla continuità di servizi critici.

L'architettura normativa del Perimetro è stata definita progressivamente dai DPCM attuativi, che di-

sciplinano criteri di individuazione dei soggetti inclusi, misure di sicurezza, obblighi di notifica degli incidenti e valutazione/certificazione delle forniture ICT, riconoscendo all'Agenzia per la Cybersicurezza Nazionale (ACN) il ruolo di autorità di riferimento per coordinamento, vigilanza e attuazione delle misure di sicurezza a livello nazionale. **Nel rapporto con la Direttiva (UE) 2022/2555 (NIS2), il Perimetro si colloca su un piano di integrazione rafforzata: i soggetti inclusi sono spesso anche destinatari degli obblighi NIS2, ma risultano assoggettati a misure più stringenti**, in particolare sulla sicurezza delle catene di approvvigionamento tecnologico e sui poteri di intervento pubblico sulle forniture.

Per il settore finanziario, il coordinamento con il Regolamento (UE) 2022/2554 (DORA) assume rilievo specifico. **Le entità che rientrano sia nell'ambito di applicazione di DORA sia nel Perimetro nazionale operano in un contesto di doppia rilevanza normativa**: DORA come disciplina settoriale speciale in materia di resilienza operativa digitale del sistema finanziario, il Perimetro come strumento di sicurezza nazionale che attribuisce ad ACN e alla Presidenza del Consiglio dei ministri poteri di valutazione preventiva, prescrizione e, nei casi più gravi, interdizione delle forniture ICT critiche.

Questa relazione non determina una mera sovrapposizione di obblighi, ma una complementarità funzionale: mentre DORA presidia il rischio operativo e sistemico del settore finanziario, il Perimetro rafforza il controllo sulle componenti tecnologiche strategiche, in continuità con la logica dei poteri speciali dello Stato (golden power) estesa al dominio cibernetico. Il GDPR continua a svolgere un ruolo trasversale, poiché gli obblighi di sicurezza del trattamento e di notifica delle violazioni dei dati personali restano pienamente applicabili ai soggetti inclusi nel Perimetro, imponendo un coordinamento accurato tra i flussi di segnalazione verso ACN, autorità settoriali e autorità di protezione dei dati.

Nel complesso, **il Perimetro di sicurezza cibernetica nazionale si inserisce in un sistema multilivello in cui norme nazionali ed europee operano secondo logiche di specialità, integrazione e coordinamento**. La sua efficacia dipende dalla capacità dei soggetti coinvolti di sviluppare modelli di governance unitaria che coniughino resilienza operativa digitale, sicurezza nazionale e tutela dei diritti fondamentali, così che il Perimetro non si traduca in un ulteriore fattore di frammentazione, ma in un presidio avanzato della postura di sicurezza dell'ordinamento italiano nel quadro europeo della cybersicurezza.

7. Considerazioni conclusive

L'analisi del rapporto tra DORA, NIS2, GDPR e disciplina nazionale evidenzia come la cybersecurity non possa più essere ricondotta a un perimetro esclusivamente regolamentare, né a una sommatoria di obblighi settoriali da adempiere in modo formalistico. Emerge, piuttosto, un dominio giuridico e organizzativo molto più ampio, nel quale le fonti normative costituiscono solo uno degli elementi di un sistema complesso, dinamico e strutturalmente interconnesso.

In questa prospettiva, **DORA rappresenta il fulcro della disciplina settoriale per le entità finanziarie**, offrendo un quadro unitario e coerente di obblighi in materia di resilienza operativa digitale. **La sua funzione non è però quella di "chiudere" il perimetro della cybersecurity, bensì di collocarsi in un contesto più ampio**, nel quale continuano a operare – secondo logiche di specialità, complementarità e integrazione – la normativa orizzontale NIS2, il GDPR, le discipline nazionali di sicurezza cibernetica (come il Perimetro di sicurezza cibernetica nazionale), nonché ulteriori strumenti di soft law, standard tecnici, linee guida e prassi di settore.

Da questo intreccio multilivello prende forma un **vero e proprio ecosistema normativo della cybersecurity, che non si fonda su una gerarchia lineare di fonti, ma su una rete di regole parzialmente integrate, spesso eterogenee per finalità, ambito soggettivo e logiche di intervento**. DORA presidia la stabilità e la continuità del sistema finanziario; la NIS2 tutela la sicurezza delle reti e dei sistemi informativi in una prospettiva intersettoriale; il GDPR protegge i diritti fondamentali delle persone fisiche attraverso la sicurezza del trattamento dei dati; il Perimetro nazionale e i poteri speciali dello Stato rispondono a esigenze di sicurezza e sovranità digitale. Ciascuna di queste discipline opera su un piano distinto, ma nessuna può dirsi autosufficiente.

Ne consegue che la cybersecurity non coincide con il mero rispetto delle singole norme, ma si configura come funzione strategica trasversale che attraversa governance aziendale, modelli organizzativi, gestione del rischio, relazioni con i fornitori, cultura interna e processi decisionali. L'adempimento regolamentare rappresenta il livello minimo di presidio, che per essere effettivo deve tradursi in capacità di integrazione tra obblighi giuridici, misure tecniche e consapevolezza organizzativa.

In tale contesto, **il coordinamento normativo assume un rilievo centrale: il rischio principale non è più**

vedi l'articolo online

l'assenza di regole, ma la loro frammentazione applicativa, cui la proposta di Digital Omnibus cerca di porre rimedio razionalizzando un sistema altrimenti esposto a duplicazioni, incoerenze e oneri sproporzionati per gli operatori. Per le entità finanziarie – e, più in generale, per i soggetti operanti in settori critici – la sfida non è stabilire quale norma prevalga, ma costruire modelli di compliance e di governance capaci di leggere e governare l'ecosistema nel suo complesso, superando un approccio silos-based in favore di una visione integrata che riconosca la cybersecurity come fattore strutturale di resilienza, fiducia e competitività.

In definitiva, **la cybersecurity emerge come spazio giuridico e organizzativo che eccede la dimensione normativa in senso stretto e si configura come terreno di convergenza tra diritto, tecnologia e strategia**. In questo ecosistema, la qualità del coordinamento – tra norme, livelli di governo, autorità di vigilanza e funzioni aziendali – diventa essa stessa una componente essenziale della sicurezza.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it