DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Finanza digitale: le novità del Regolamento DORA

30 Marzo 2023

Vittorio Pietroluongo, Lener & Partners

Vittorio Pietroluongo, Lener & Partners

Studio legale
Lener & Partners

1. Il Digital Operational Resilience Act (Regolamento DORA)

Le tecnologie applicate ai servizi finanziari hanno ormai creato un nuovo ecosistema, fluido e in costante mutamento, che ha comportato, però, la progressiva disintermediazione delle entità finanziarie "classiche" e la conseguente flessione dei livelli di *cybersecurity*.

La sicurezza informatica, infatti, non può più essere considerata un aspetto ancillare; essa rappresenta ormai un elemento fondante delle infrastrutture e dei servizi finanziari. È sorta, quindi, la necessità di sviluppare nuovi modelli di sicurezza per tenere il passo con i nuovi ecosistemi finanziari e tecnologici.

Al fine di rafforzare la sicurezza informatica delle società finanziarie, dunque, il 28 novembre 2022, il Consiglio dell'Unione Europea ha adottato del Regolamento (UE) 2022/2554, c.d. Regolamento DORA.

2. La cornice europea: il rapporto tra il Regolamento Dora e la Direttiva NIS2

Pubblicato in Gazzetta Ufficiale dell'Unione Europea il 27 dicembre 2022, unitamente alla *Direttiva NIS2* e alla *Direttiva CER (Cyber Entity Resilience),* il Regolamento DORA si inserisce nell'ambito delle iniziative europee relative alla sicurezza digitale volte a sostenere ed accrescere il potenziale della finanza digitale in termini di innovazione e concorrenza.

In particolare, con il Regolamento DORA è stato previsto il rafforzamento delle misure di sicurezza informatica del settore finanziario, assicurando così agli operatori coinvolti[1] di prevenire e contrastare la crescente minaccia di attacchi informatici.

Già nel 2016, infatti, il Parlamento europeo e il Consiglio avevano adottato la direttiva NIS (sostituita

1 In particolare, il Regolamento DORA si rivolge a un ampio novero di operatori finanziari, quali: enti creditizi; istituti di pagamento; prestatori di servizi di informazione sui conti; istituti di moneta elettronica; imprese di investimento; fornitori di servizi per le cripto-attività; depositari centrali di titoli; controparti centrali; sedi di negoziazione; repertori di dati sulle negoziazioni; gestori di fondi di investimento alternativi; società di gestione; fornitori di servizi di comunicazione dati; imprese di assicurazione e di riassicurazione; intermediari assicurativi, intermediari riassicurativi e intermediari assicurativi a titolo accessorio; enti pensionistici aziendali o professionali; agenzie di *rating* del credito; amministratori di indici di riferimento critici; fornitori di servizi di *crowdfunding*, repertori di dati sulle cartolarizzazioni; e anche ai fornitori di servizi di tecnologie dell'informazione e della comunicazione (ICT).

vedi l'articolo online

dalla NIS2) sulla sicurezza delle reti e dell'informazione, finalizzata a rafforzare il livello generale di sicurezza informatica nell'UE per i fornitori di infrastrutture critiche che si applicava agli operatori di servizi essenziali in sette settori, compreso il settore finanziario.

Nello specifico, la NIS rendeva obbligatoria l'adozione di misure di sicurezza rinforzate per gli operatori di tali settori, individuati a livello nazionale da criteri stabiliti dalla NIS stessa. Nel settore finanziario solo i grandi istituti di credito, le sedi di negoziazione, le imprese di assicurazione e le controparti centrali rientrano nell'ambito di applicazione della NIS.

La direttiva NIS2, adottata definitivamente nel novembre 2022, amplia l'ambito di applicazione della NIS, coprendo un maggior numero di imprese nei settori esistenti; ciò nonostante, la disciplina del Regolamento DORA comprende tutti gli intermediari finanziari, indipendentemente dalla loro rilevanza per il settore finanziario, oltre a prevedere requisiti di gran lunga più vincolanti e dettagliati.

Inoltre, il Regolamento DORA innalza il livello di armonizzazione delle componenti di "resilienza digitale", introducendo requisiti in materia di gestione del rischio ICT (*Information and Communications Technology*) e di segnalazione degli incidenti connessi alle ICT più rigorosi rispetto a quelli previsti dalla vigente normativa dell'Unione in materia di servizi finanziari.

Per questo motivo, la disciplina del Regolamento DORA è stata concepita come *lex specialis,* il considerando 16 stabilisce infatti che essa è una regola speciale, e quindi prevalente, rispetto alla NIS2. In caso di sovrapposizioni, dunque, si applicheranno le disposizioni del Regolamento DORA. In ogni caso è evidente l'importanza dell'interconnessione tra gli ecosistemi DORA e NIS2, data la sovrapposizione di obiettivi, ambiti di applicazione e regole.

3. Ambito di applicazione

Entrato in vigore il 17 gennaio 2023, il Regolamento DORA troverà applicazione il 17 gennaio 2025. Entro questa data, gli operatori finanziari e le terze parti che forniscono loro servizi relativi alle ICT dovranno conformarsi ai requisiti previsti adottando numerose misure di sicurezza, oltre a predisporre strumenti idonei a garantire una rendicontazione continua e costante del livello di sicurezza richiesto.

In particolare, le previsioni dettate dal Regolamento DORA hanno ad oggetto:

- il consolidamento dei compiti e delle responsabilità degli organi di gestione delle società finanziarie coinvolte, con particolare riguardo agli *standard* di sicurezza informatici e all'adattamento delle relative politiche di controllo;

- l'affidamento ad un organo di controllo indipendente delle responsabilità della gestione e sorveglianza dei rischi ICT, oltre alla possibilità di esternalizzare la funzione *compliance* in materia di gestione dei rischi informatici; e

- il rafforzamento delle misure volte a garantire la continuità operativa dell'ente finanziario, mediante la predisposizione di analisi volte a prevedere gli impatti che eventuali gravi criticità nelle funzioni commerciali, nei processi di supporto, nelle dipendenze da terzi e/o nei patrimoni informativi individuati e censiti, nonché nelle loro interdipendenze possono avere sulle attività aziendali[2].

4. Adempimenti e obblighi per gli operatori finanziari: cosa aspettarsi

L'entrata in vigore del Regolamento DORA, dunque, ha imposto agli operatori finanziari coinvolti di predisporre un piano di adeguamento che renda il più semplice possibile il recepimento della nuova disciplina, visti i numerosi adempimenti ai quali gli operatori finanziari dovranno far fronte.

In tal senso, molti dei nuovi requisiti del Regolamento DORA richiederanno l'adozione di un approccio attivo e informato, che contempli lo svolgimento di una serie di attività.

L'articolo 4 del DORA stabilisce che gli enti finanziari attuino le norme secondo il principio di "*proporzionalità*", in considerazione delle dimensioni, della natura, dell'entità e della complessità dei loro servizi, attività e operazioni e il loro profilo di rischio complessivo

Sebbene questo principio sia una regola generale, che dovrebbe essere adottata nel recepimento di tutti gli atti legislativi di diritto europeo, il legislatore ha avvertito la necessità di ribadire il concetto

2 C.d. *Business Impact Analysis (BIA).*

vedi l'articolo online

nell'art. 4. Questo accorgimento è un segnale importante che le disposizioni del Regolamento DORA dovranno essere applicate in maniera completa, in base ad una specifica analisi di profili di rischio adeguata rispetto alla dimensione dell'azienda, perseguendo la finalità di mantenere l'intero settore finanziario sicuro dalle *"cyber minacce"*.

Dall'analisi complessiva del dettato normativo del Regolamento DORA, infatti, emergono numerosi obblighi cui gli operatori finanziari devono adempiere, tra i quali i più rilevanti prevedono di:

- adottare un quadro di *governance* e organizzazione interna che garantisca un controllo efficace e prudente di tutti i rischi ICT;
- adottare un piano per la gestione dei rischi informatici, stabilendo precise regole di gestione del rischio relativi alle tecnologie ICT, creando un *ICT Risck Managment Framework* e definendo una strategia di resilienza digitale;
- identificare e classificare gli incidenti connessi ai fornitori ICT e le minacce informatiche;
- creare un sistema di segnalazione e di gestione degli incidenti e dei rischi informatici, anche derivanti da terzi;
- accertare le competenze e le capacità necessarie per la definizione e gestione dei test di resilienza;
- svolgere test di resilienza digitale;
- porre in essere i controlli di sicurezza sulla propria infrastruttura digitale mediante l'applicazione specifiche misure tecniche, quali ad esempio la crittografia, l'autenticazione multi-fattore, il controllo degli accessi, lo svolgimento di audit, l'implementazione di sistemi di monitoraggio, di gestione degli eventi e di piani di risposta agli incidenti; e
- prevedere protocolli di *information sharing*.

In aggiunta, la procedura di adeguamento dovrà necessariamente allinearsi con le altre discipline in materia di *cybersecurity*. Infatti, l'impianto del Regolamento DORA ha punti di contatto con diverse altre discipline sia a livello europeo[3] che nazionale[4].

Al tempo stesso, anche le autorità europee di vigilanza ("***AEV***")[5] dovranno elaborare standard tecnici *ad hoc* e vigilare sul rispetto del regolamento.

Il Regolamento DORA non incide sulle responsabilità degli Stati membri per quanto riguarda le funzioni statali essenziali in materia di pubblica sicurezza, difesa e sicurezza cibernetica nazionale in conformità al diritto dell'Unione.

5. Approfondimento: la sorveglianza dei fornitori di servizi ICT

Come sottolineato da diversi studi di settore[6], la resilienza operativa dei fornitori servizi ICT è una questione di primaria importanza per il settore finanziario dell'Unione Europea, che ne fa sempre più uso. Il Regolamento DORA affronta specificamente questo problema e, in particolare, la propensione delle società finanziarie a esternalizzare le proprie infrastrutture informatiche a fornitori di servizi ICT.

In primo luogo, i fornitori di servizi ICT che sono ritenuti critici per le entità finanziarie saranno designati[7] dalle AEV. Il processo di designazione si baserà sulla continuità e sulla qualità dei servizi finanziari offerti, anche in considerazione dell'impatto sistemico che potrebbero avere eventuali guasti operativi di grande entità.

Da questo presupposto, si può dedurre che saranno designati soprattutto i fornitori di servizi ICT più

3 Come ad es.: *MIFID II*, *GDPR*, *Basel Committee's 2021 Principles on Operational Resilience*, *EIOPA Guidelines*, oltre alle già citate *Direttiva NIS2* e alla *Direttiva CER*.

4 Ovvero, il PSNC (Perimetro di Sicurezza Nazionale Cibernetica), la *Circolare 285 di Banca d'Italia* e il *Regolamento IVASS*.

5 Quali: *l'EBA (Autorità bancaria europea), l'ESMA (Autorità europea degli strumenti finanziari e dei mercati) e l'EIOPA (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali).*

6 In particolare, il Financial Stability Board (FSB) nel rapporto *BigTech in finance -Market developments and potential financial stability implications*, del 9 dicembre 2019, evidenzia come le entità finanziarie affidino ormai quasi esclusivamente i servizi ICT avanzati a fornitori terzi, definiti *Critical Third Party Providers* (*CTPP*).

7 La designazione si fonda sulla valutazione di tutti i criteri indicati dall'art 31, comma 2, Regolamento DORA.

grandi (c.d. *Big Tech*)[8], a seconda del numero di banche e assicurazioni di rilevanza sistemica globale che si affidano ai loro servizi.

In una seconda fase, per ogni fornitore designato sarà individuata un'AEV a presidio della vigilanza.

Il coinvolgimento di tutte e tre le AEV desta perplessità circa la capacità di sviluppare rapidamente le competenze e le nuove infrastrutture amministrative per ognuna delle AEV. In ogni caso, sembra lecito aspettarsi che nella maggior parte dei casi sarà l'EBA ad avere il maggior numero di incarichi come supervisore, considerato che le banche rappresentano il gruppo più numeroso e di maggiore rilevanza sistemica come utenti di servizi ICT.

L'autorità di vigilanza incaricata dovrà principalmente richiedere informazioni, condurre ispezioni generali e formulare raccomandazioni ai fornitori di servizi ICT, i quali, a loro volta, dovranno dimostrare di poter garantire di essere protetti da rischi operativi di grave entità e la stabilità e la continuità dei servizi forniti alle società finanziarie.

La AEV incaricata, inoltre, valuterà anche il processo di gestione del rischio, i presidi di *governance*, i meccanismi per la portabilità dei dati e i programmi di test dei sistemi ICT.

Una volta conclusa la fase di indagine, le AEV dovranno formulare raccomandazioni in ordine alle eventuali criticità emerse durante le ispezioni e fornire informazioni circa la loro soluzione. Sarà, poi, compito delle autorità di vigilanza nazionali competenti dar seguito alle raccomandazioni, informando i soggetti interessati dei rischi rilevati e assicurandosi che vengano prese le adeguate contromisure.

Le autorità di vigilanza nazionali competenti potranno, inoltre, adottare provvedimenti nei confronti delle imprese finanziarie sottoposte a vigilanza in caso di mancato recepimento delle raccomandazioni. Come misura di ultima istanza, infatti, le AEV avranno la facoltà di imporre alle entità finanziarie di sospendere temporaneamente l'utilizzo o direttamente di interrompere il rapporto di fornitura di un servizio fino a quando i rischi identificati non saranno stati risolti, e nel caso in cui questi ultimi dovessero risultare insormontabili, di risolvere i loro contratti con il fornitore interessato.

8 Un elenco non esaustivo di aziende BigTech: Alibaba, Amazon, Apple, Baidu, eBay, Facebook, Google, Microsoft, Tencent.

6. Conclusioni

Sebbene l'intervento di vigilanza in relazione ai fornitori di servizi ICT avvenga ancora indirettamente attraverso i soggetti vigilati, il regime previsto dal Regolamento DORA è un grande passo avanti per monitorare al meglio i potenziali rischi derivanti dal mondo dei servizi ICT.

Se, da una parte, infatti, la rilevante interconnessione digitale tra le entità finanziarie ha reso possibile la creazione di un mercato unico, dove le imprese finanziarie sono libere di operare in tutto il territorio dell'Unione, dall'altra si è venuto a creare anche un rapporto di dipendenza reciproca che, allo stato attuale, cela rilevanti vulnerabilità.

I problemi dovuti a dei servizi ICT, infatti, potrebbero scatenare un "effetto domino", potenzialmente capace di coinvolgere l'intera rete, proprio a causa dell'interdipendenza tra gli enti che caratterizza il mercato finanziario.

Tanto rappresentato, il quadro fornito dal Regolamento DORA, che stabilisce in maniera chiara le priorità in materia di governance ICT, reporting e test, sembra essere indispensabile. Sebbene alcune disposizioni del Regolamento DORA siano piuttosto restrittive, infatti, l'approccio basato sulla costante e puntuale analisi del rischio porterà a un'applicazione equilibrata dei requisiti previsti.

Si sottolinea, a tal proposito, come diverse disposizioni responsabilizzino gli istituti finanziari tanto da "costringerli" a superare un approccio puramente passivo degli adempimenti richiesti, rendendoli parte attiva del processo di protezione della sicurezza informatica.

In conclusione, il processo di supervisione europeo sui fornitori terzi di servizi ICT critici previsto dal Regolamento DORA è la risposta giusta alla tendenza in atto delle entità finanziarie a esternalizzare la propria infrastruttura IT. L'adozione di una cultura della sicurezza informatica e la predisposizione di adeguati strumenti di protezione rappresentano, infatti, una condizione essenziale per garantire la sostenibilità e la competitività del settore finanziario nella nuova era digitale.

Se, dunque, questo modello di vigilanza avrà successo, potrebbe in futuro anche rivestire un ruolo pionieristico per altri settori.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it