La Comunicazione - Note, Recensioni e Notizie n. 69
Anno 2025

Resilienza operativa digitale: Regolamento 2022/2554 (DORA)

Digital operational resilience: Regulation 2022/2554 (DORA)

Giancarlo Butti ♦

♦ ISACA – Milano

Sommario

Il Regolamento DORA (Digital Operational Resilience Act), entrato in vigore nel gennaio 2023 e pienamente operativo dal gennaio 2025, rappresenta un'importante iniziativa dell'UE per rafforzare la resilienza operativa digitale delle entità finanziarie contro i rischi cyber. Sebbene rivolto principalmente al settore finanziario, coinvolge direttamente anche i fornitori ICT delle entità finanziarie e la loro catena di subfornitura.

Il concetto chiave della resilienza operativa digitale si riferisce alla capacità di garantire la resilienza in presenza di perturbazioni, attraverso un'efficace gestione dei rischi legati all'ICT. Il Regolamento 2022/2554 si colloca in un contesto normativo che include altre iniziative come la NIS2 e il Cybersecurity Act.

Il Regolamento introduce obblighi per le entità finanziarie su cinque pilastri principali: gestione del rischio ICT, segnalazione degli incidenti, test di resilienza digitale, gestione dei rischi legati ai fornitori e condivisione delle informazioni. Le istituzioni finanziarie devono adottare framework di gestione robusti, testare regolarmente la resilienza e stabilire contratti con i fornitori ICT che rispettino i requisiti normativi. Tuttavia, i fornitori sono impattati solo contrattualmente, non normativamente, salvo siano designati come fornitori critici.

Il Regolamento 2022/2554 non è esente da difetti, a cominciare dell'iter normativo scelto per l'emissione della normativa integrativa, o la presenza di errori sia di natura formale che sostanziale nel testo del Regolamento.

Abstract

The Dora Regulation (Digital Operational Resilience Act), which came into force in 2023 and fully operational since 2025, represents an important EU initiative to strengthen the digital operational resilience of financial entities against cyber risks. Although aimed primarily at the financial sector, I also involves ICT suppliers and their subcontracting chain.

The key concept of digital operational resilience refers to the ability to guarantee resilience in the presence of perturbations, through effective management of the risks related to tics (information and communication technologies). DORA is part of a regulatory framework that includes other initiatives such as NIS2 and the Cybersecurity Act.

The regulation introduces obligations for financial entities on five main pillars: ICT risk management, accident reporting, digital resilience test, risk management related to suppliers and information sharing. Financial institutions must adopt robust management framework, regularly test resilience and establish contracts with ICT suppliers that comply with regulatory requirements. However, suppliers are only contractually impactful, not normally, unless they are designated as critics.

Dora is not exempt from defects, starting with the regulatory process chosen for the issue of the supplementary legislation, or the presence of both formal and substantial errors in the text of the regulation.

Keyword

Resilience, cybersecurity, supply chain, risk, business continuity

1 - Introduzione

Entrato in vigore nel gennaio del 2023 e pienamente operativo dal gennaio 2025, il **REGOLAMENTO (UE) 2022/2554 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n.**

909/2014 e (UE) 2016/1011, meglio noto come Regolamento DORA , costituisce una importante iniziativa normative a livello comunitario, tesa ad aumentare la resilienza delle entità finanziarie rispetto ai crescenti rischi del mondo cyber.

In realtà, al di là della apparente applicazione al settore finanziario, il Regolamento 2022/2554 si applica direttamente o indirettamente ad una platea veramente molto vasta di soggetti, la maggior parte dei quali non è tutt'oggi cosciente di essere fra i destinatari della normativa.

Ma cosa si intende per resilienza?

Le definizioni sono molteplici, come ci ricorda il dizionario Treccani, fra le quali quella che più si avvicina a Regolamento 2022/2554 è la seguente:

3. In psicologia, la capacità di reagire di fronte a traumi, difficoltà, ecc.

Infatti la definizione che l'articolo 3 del Regolamento 2022/2554 dà della resilienza è la seguente:

«resilienza operativa digitale»: la capacità dell'entità finanziaria di costruire, assicurare e riesaminare la propria integrità e affidabilità operativa, garantendo, direttamente o indirettamente tramite il ricorso ai servizi offerti da fornitori terzi di servizi TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza dei sistemi informatici e di rete utilizzati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità, anche in occasione di perturbazioni;

Tale definizione si ritrova presente, con poche differenze, anche in normative non comunitarie, quali ad esempio:

UK Prudential Regulation Authority

…the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover, and learn from operational disruptions.

US: Sound Practices to Strengthen Operational Resilience

…the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard.

o all'interno di standard ISO quali l'**ISO 22316:2017 - Security and resilience — Organizational resilience — Principles and attributes**

Organizational resilience is the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper

L'esistenza di normative che trattano lo stesso tema al di fuori dell'UE non è da sottovalutare, in quanto tali normative, precedenti alla pubblicazione del Regolamento 2022/2554, possono essere utilizzate proficuamente come guida alla sua corretta implementazione, in quanto generalmente accompagnate da documenti tecnici che traducono, nella pratica operativa, i principi espressi nella loro definizione.

2 - Il contesto normativo

Il Regolamento 2022/2554 nasce nell'ambito di un contesto che ha visto, negli ultimi anni, il tentativo da parte dell'UE, di regolamentare il mondo digitale e le nuove tecnologie, attraverso il rilascio di numerose normative, quali: il **Digital Services Act**, il **Digital Markets Act**, il **Markets in Crypto-Assets Regulation**, l'**Artificial Intelligence Act**, il **Data Governance Act**, il **Data Act**…

Più specificatamente nel mondo della sicurezza digitale, contestualmente al Regolamento 2022/2554, è stata rilasciata, ad esempio, la **Direttiva 2022/2555 (NIS2)**, ed in precedenza il **Cybersecurity Act**…

Facendo riferimento alla specifica normativa del settore finanziario, il Regolamento 2022/2554 (e le normative ad esso collegate) è molto simile a normative pre esistenti emesse in particolare da **EBA** (European Banking Authority), quali gli *Orientamenti in materia di esternalizzazione* o gli *Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza)* …

Di fatto i Regolamenti delegati che costituiscono una integrazione del Regolamento 2022/2554 fanno ampio riferimento in particolare ai documenti prodotti da EBA.

3 – Le motivazioni di DORA

Il Regolamento 2022/2554 nasce per risolvere una serie di problematiche individuate dalla Commissione europea, che comprendono:

- la regolamentazione normativa relativa alla gestione dei rischi ICT risulta frammentata, priva di requisiti specifici e caratterizzata da disomogeneità tra i diversi settori finanziari
- non esiste una visione chiara e completa sulla frequenza e la gravità degli incidenti, principalmente a causa dell'inefficacia del loro monitoraggio
- gli obblighi di segnalazione risultano spesso complessi, incoerenti e duplicati, creando difficoltà operative
- la condivisione delle informazioni sulle minacce rimane limitata e poco efficace
- i risultati dei test di sicurezza non sono riconosciuti a livello transfrontaliero, ostacolando un approccio unitario
- esistono carenze significative nella valutazione della capacità di resilienza
- le istituzioni finanziarie incontrano difficoltà nel garantire la conformità alle normative vigenti
- i rischi legati alla catena di fornitura ICT sono in aumento, soprattutto in relazione alla crescente dipendenza dai fornitori di servizi cloud.

4 - Architettura della normativa

Il Regolamento 2022/2554 ha un'architettura complessa in quanto, ad integrazione del documento principale del Regolamento, organizzato in 106 considerando e 64 articoli, è prevista l'emissione, a vario titolo, di altri 16 documenti.

La maggior parte di questi, dieci per la precisione, sono direttamente indirizzati alle entità finanziarie, e comprendono otto **RTS** (Regulatory Technical Standards) e due **ITS** (Implementing Technical Standards).

Alla redazione di questi documenti hanno partecipato le tre **ESA** (European Supervisory Authorities), costituite da **EBA**, **EIOPA** (European Insurance and Occupational Pensions Authority) ed **ESMA** (European Securities and Markets Authority) congiuntamente a **ENISA** (European Union Agency for cybersecurity), ed hanno la finalità di specificare, in una forma molto più analitica, i requisiti normativi necessari a garantire una adeguata resilienza operativa digitale.

Gli altri documenti sono costituiti da Linee guida ed altre tipologie di documenti.

Nella loro forma consolidata, questi documenti sono stati emessi sotto forma di Regolamenti delegati (al momento della prima stesura di questo articolo non tutti i documenti sono stati rilasciati nella loro forma definitiva).

Non è la prima volta che il legislatore europeo emette una normativa di alto livello, accompagnata da documenti tecnici di maggior dettaglio, con la finalità di realizzare un atto legislativo neutro rispetto alla evoluzione tecnologica e quindi valido sia oggi, sia in un prossimo futuro.

Anche l'architettura adottata per il GDPR è la medesima, ma la scelta del legislatore in quel caso è stata diversa e, probabilmente, molto più efficace.

Con il GDPR la normazione di secondo livello non è stata mantenuta a livello centralizzato, ma è stata in qualche modo delegata all'**EDPB** (European Data Protection Board), il quale ha una sorta di potere legislativo ed in effetti pubblica, con una frequenza rilevante, linee guida ed altri documenti che traducono in pratica operativa (aggiornata e contestuale alle tecnologie emergenti) i requisiti del GDPR.

La scelta del legislatore sul Regolamento 2022/2554, basata su un iter legislativo tradizionale, che porta alla emissione di Regolamenti delegati che a tutti gli effetti costituiscono una integrazione del Regolamento 2022/2554, si sta rilevando da subito poco efficace e poco flessibile, e caratterizzata da lunghi tempi di emissione.

Ne è una prova il fatto che al momento della prima stesura di questo articolo, meno di 15 giorni dalla piena efficacia del Regolamento 2022/2554, non è stato ancora rilasciato un Regolamento delegato fondamentale, quello sui subfornitori.

RTS ed ITS, sono stati realizzati con un lungo processo che ha comportato l'emissione di una prima bozza da parte delle ESA, finalizzata ad una consultazione pubblica circa il loro contenuto.

L'analisi dei commenti ricevuti ha portato le ESA ad una revisione delle prime bozze ed alla emissione di una seconda bozza finale la quale, successivamente, è stata emessa (non senza ulteriori modifiche) come atto legislativo finale da parte della Commissione europea.

Un processo durato circa 18 mesi, che mal si concilia con i tempi dell'evoluzione tecnologica.

Per tale motivo, a differenza delle linee guida emesse dall'EDPB, anche questa normativa integrativa si mantiene ad un livello alto, di neutralità tecnologica, e quindi lascia spazio (e responsabilità) alle singole entità finanziarie, circa la sua corretta implementazione.

Il livello di dettaglio del Regolamento 2022/2554 è comunque enormemente maggiore di quello proposto dalla NIS2, la quale fornisce limitatissime informazioni in merito a come implementare i vari requisiti normativi.

Considerando che dal punto di vista normativo, il Regolamento 2022/2554 costituisce un atto giuridico settoriale rispetto alla NIS2, è possibile utilizzare il Regolamento 2022/2554 ed i relativi RTS ed ITS come buone pratiche a cui fare riferimento per implementare la NIS2.

5 - Ambito di applicazione

Il Regolamento 2022/2554 è probabilmente la prima normativa che ricomprende fra i soggetti destinatari della stessa, non soltanto i diretti interessati (le entità finanziarie), ma anche i loro fornitori ICT, a qualunque livello della catena di fornitura questi si trovino.

È per tale motivo che, come si accennava nei paragrafi precedenti, il perimetro di applicazione del Regolamento 2022/2554 è particolarmente ampio ed è quindi molto probabile che, una qualunque azienda di servizi ICT, possa essere coinvolta nel rispetto dei requisiti del Regolamento, anche se non ha fra i suoi clienti diretti una entità finanziaria.

Prima di continuare chiariamo cosa il Regolamento 2022/2554 intenda per entità finanziaria e per fornitore ICT.

Per quanto attiene il primo termine, l'articolo 2 del Regolamento 2022/2554 identifica una ventina di tipologie diverse di soggetti (dagli enti creditizi alle imprese di assicurazione e di riassicurazione, dai gestori di fondi di investimento alternativi agli enti pensionistici aziendali o professionali …, definendoli collettivamente entità finanziarie).

È a loro che si applica principalmente la normativa, senza alcuna distinzione fra le varie tipologie di soggetti, ma limitandosi a introdurre delle semplificazioni solo per quei soggetti le cui "dimensioni" soddisfano determinati parametri.

Per fornitore terzo di servizi ICT (TIC è il termine usato dal Regolamento 2022/2554), si intende un'impresa che fornisce servizi ICT.

Il **Final Report On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554**, identifica i servizi ICT riportati nella Tabella 1.

Tabella 1. Tipologia di servizi ICT

Type of ICT services
1. ICT project management
2. ICT Development
3. ICT help desk and first level support
4. ICT security management services
5. Provision of data
6. Data analysis
7. ICT, facilities and hosting services (excluding Cloud services)
8. Computation
9. Non-Cloud Data storage
10. Telecom carrier
11. Network infrastructure
12. Hardware and physical devices
13. Software licencing(excluding SaaS)
14. ICT operation management (including maintenance)
15. ICT Consulting
16. ICT Risk management
17. Cloud services: IaaS
18. Cloud services: PaaS
19. Cloud services: SaaS

Entrambe le categorie di soggetti devono sottostare al Regolamento 2022/2554, ma in modo molto differente.

Infatti, secondo l'articolo 1 del Regolamento 2022/2554, alle entità finanziarie si applicano obblighi in materia di:

- *gestione dei rischi delle tecnologie dell'informazione e della comunicazione (TIC);*
- *segnalazione alle autorità competenti degli incidenti gravi connessi alle TIC e notifica, su base volontaria, delle minacce informatiche significative;*
- *segnalazione alle autorità competenti, da parte delle entità finanziarie di cui all'articolo 2, paragrafo 1, lettere da a) a d), di gravi incidenti operativi o relativi alla sicurezza dei pagamenti;*
- *test di resilienza operativa digitale;*
- *condivisione di dati e di informazioni in relazione alle vulnerabilità e alle minacce informatiche;*
- *misure relative alla solida gestione dei rischi informatici derivanti da terzi.*

Per contro ai fornitori ICT, ed alle entità finanziarie sono prescritti, congiuntamente:

- *obblighi relativi agli accordi contrattuali stipulati tra fornitori terzi di servizi TIC ed entità finanziarie.*

In altre parole, dal punto di vista strettamente normativo, l'unico obbligo dei fornitori ICT è quello di formalizzare mediante un contratto scritto il loro rapporto con le entità finanziarie.
Di fatto non sono previste sanzioni per i fornitori, salvo che non si tratti di fornitori critici.
La definizione di fornitore critico riportata nell'articolo 3 del Regolamento 2022/2554 è la seguente *"fornitore terzo critico di servizi TIC»: un fornitore terzo di servizi TIC designato come critico in conformità dell'articolo 31",* e non va confuso con il fatto che un fornitore possa risultare particolarmente significativo per una specifica entità finanziaria.
I fornitori critici sono soggetti che hanno caratteristiche tali da essere considerati rilevanti a livello sistemico, e per i quali il Regolamento 2022/2554 introduce un controllo diretto da parte delle Autorità di Vigilanza.
Per tali soggetti sono previste sanzioni relativamente a violazioni in merito ai loro obblighi nei confronti delle Autorità di Vigilanza.

6 –I pillar di DORA

Sintetizzando i contenuti dell'articolo 1 prima citato, i pillar del Regolamento 2022/2554 a cui devono sottostare le entità finanziarie sono i seguenti:

- gestione del rischio ICT
- segnalazione degli incidenti connessi all'ICT
- test di resilienza operativa digitale
- rischi relativi all'ICT derivanti da terzi
- condivisione delle informazioni.

Più dettagliatamente, per quanto attiene la gestione del rischio ICT, le entità finanziarie devono prevedere:

- la creazione di un sistema di governance interna: sviluppo di strutture e controlli che garantiscano una gestione efficace e prudente dei rischi associati all'ICT
- ruoli e responsabilità dell'organo direttivo: assegnazione di compiti specifici per la supervisione e gestione dei rischi ICT
- adozione di un framework strutturato: implementazione di un modello completo e robusto per affrontare i rischi legati all'ICT
- utilizzo di soluzioni resilienti: impiego di strumenti e sistemi progettati per minimizzare gli impatti derivanti dai rischi ICT
- monitoraggio e analisi dei rischi: identificazione continua delle principali fonti di vulnerabilità nell'ambito ICT
- pianificazione della continuità operativa: definizione di politiche e sistemi di recovery per gestire eventi critici legati all'ICT
- implementazione di misure preventive: adozione di strategie di protezione e prevenzione efficaci
- rilevamento di attività sospette: capacità di individuare tempestivamente comportamenti o azioni anomale

- risorse dedicate e personale specializzato: disponibilità di strumenti e competenze per analizzare vulnerabilità, minacce, attacchi informatici e incidenti, valutando i loro effetti sulla resilienza digitale
- revisione degli incidenti e miglioramento continuo: analisi delle esperienze passate, condivisione delle lezioni apprese, aggiornamento delle tecnologie, formazione e sensibilizzazione del personale
- piani di comunicazione efficaci: sviluppo di strategie chiare e mirate per mantenere informati tutti gli stakeholder.

Relativamente ai rischi ICT ulteriori specificazioni sono contenute nel relativo Regolamento delegato, il quale sviluppa numerosi aspetti legati alla gestione della sicurezza quali, ad esempio:

- sviluppo di politiche e strumenti per la sicurezza ICT: creazione di linee guida, procedure, protocolli e strumenti per garantire la protezione delle risorse informatiche
- protezione delle risorse IT aziendali: monitoraggio continuo e difesa dei sistemi contro minacce interne ed esterne
- sicurezza e crittografia dei dati: implementazione di tecniche per proteggere l'integrità, la riservatezza, la disponibilità e l'autenticità delle informazioni
- ottimizzazione delle prestazioni dei sistemi: gestione della capacità e monitoraggio delle performance per garantire efficienza e affidabilità
- gestione delle vulnerabilità: identificazione, valutazione e aggiornamento dei sistemi per mitigare i rischi
- monitoraggio delle attività IT: registrazione e analisi dei log per rilevare anomalie e garantire la conformità
- protezione delle infrastrutture di rete: prevenzione di accessi non autorizzati e difesa contro le minacce esterne
- gestione dei progetti ICT: supervisione dei progetti e dei cambiamenti per garantire la coerenza con gli obiettivi aziendali

- acquisizione e manutenzione dei sistemi ICT: gestione del ciclo di vita dei sistemi, dall'acquisto allo sviluppo fino alla manutenzione
- gestione delle modifiche ai sistemi: controllo delle variazioni nei sistemi ICT per garantire continuità e sicurezza
- sicurezza fisica e ambientale: protezione delle infrastrutture da rischi ambientali e accessi non autorizzati
- politiche per le risorse umane e gestione degli accessi: definizione di regole per controllare l'accesso alle risorse aziendali in base ai ruoli
- pianificazione della continuità operativa ICT: sviluppo e gestione di strategie per assicurare la disponibilità dei sistemi in caso di emergenza
- esecuzione di test sui piani di continuità: verifica regolare dell'efficacia dei piani per garantire la loro adeguatezza.

Nella stesura del Regolamento delegato, come chiaramente indicato nel Final Draft che ne ha anticipato la pubblicazione, le ESA si sono basate sugli standard europei e internazionali più rilevanti per la gestione dei rischi ICT. Tra questi si annoverano: le Linee guida dell'EBA sui rischi ICT e la sicurezza, quelle dell'EIOPA sulla sicurezza e governance ICT, la Direttiva NIS2, il framework NIST per la cybersecurity, la serie di standard ISO-IEC 27000, il toolkit CIRR del FSB, i Principi Fondamentali di Cybersecurity sviluppati dai Paesi del G7 per il settore finanziario, le raccomandazioni del CPMI-IOSCO sulla resilienza cibernetica delle infrastrutture di mercato finanziario e i principi del BCBS relativi alla resilienza operativa, alla gestione del rischio operativo, all'aggregazione dei dati sui rischi e alla loro rendicontazione.

Per quanto concerne gli altri aspetti del Regolamento 2022/2554, in particolare la gestione delle segnalazioni degli incidenti ICT, trattata al Capo III del Regolamento, le istituzioni finanziarie dovranno adottare un sistema strutturato per identificare e registrare gli incidenti legati all'ICT, inclusi quelli operativi e di sicurezza relativi ai pagamenti. Tali incidenti saranno classificati e valutati in base a criteri predefiniti. Gli eventi di maggiore rilevanza dovranno essere formalmente segnalati alle autorità competenti.

Le notifiche saranno standardizzate attraverso un formato unificato e dovranno comprendere rapporti preliminari, intermedi e finali. A questo proposito, nel settore bancario, la Banca d'Italia ha già pubblicato linee guida e istruzioni per l'inoltro delle segnalazioni. Inoltre, le istituzioni dovranno informare utenti e clienti ogniqualvolta un incidente abbia, o possa avere, ripercussioni negative sui loro interessi economici.

Per quanto riguarda i test di resilienza operativa digitale, le entità finanziarie saranno tenute a effettuare verifiche periodiche volte a identificare vulnerabilità, carenze o punti deboli, oltre a valutare la loro capacità di implementare rapidamente misure correttive. Questi test saranno progettati in base alla dimensione dell'entità, al profilo di rischio e al modello di business adottato.

Solo le entità più rilevanti, caratterizzate da un alto livello di maturità tecnologica, saranno obbligate a svolgere test avanzati, come penetration test basati su scenari specifici di minacce. Gli operatori che condurranno tali test dovranno rispettare i requisiti stabiliti dall'articolo 27.

Infine, in tema di condivisione delle informazioni, sarà possibile stipulare accordi tra le entità finanziarie per lo scambio di dati e dettagli relativi alle minacce informatiche.

7 – Il coinvolgimento e gli impatti sui fornitori ICT

Se l'unica obbligazione normativa per i fornitori ICT riguarda la stesura di un contratto scritto con l'entità finanziaria cliente, perché gli stessi risulterebbero fortemente impattati dal Regolamento 2022/2554?

La risposta a questa domanda è molto semplice.

Le entità finanziarie nella stesura dei loro contratti con un fornitore ICT devono necessariamente imporre una serie di condizioni, dettate principalmente dall'articolo 30 del Regolamento 2022/2554 e dal Regolamento delegato sui fornitori (alla data di prima stesura di questo articolo l'analogo regolamento sui sub fornitori, previsto dalla normativa, è disponibile solo sotto forma di final draft).

Accanto a queste clausole espressamente previste dalle normative, che vincolano i fornitori ICT, la singola entità finanziaria deve imporre una serie di clausole, senza le quali non sarebbe garantito il rispetto della normativa da parte della entità finanziaria stessa.

Ad esempio, se l'entità finanziaria deve cifrare i propri dati ed una parte di tali dati sono trattati da un fornitore ICT, ne consegue che anche il fornitore ICT dovrà cifrare questi dati.

Complessivamente il numero di clausole esplicitamente o implicitamente previste dal Regolamento 2022/2554 e dalle normative che integrano il Regolamento possono essere diverse decine.

Il fornitore ICT, se vuole continuare ad operare per l'entità finanziaria cliente, deve necessariamente sottostare a tali clausole e quindi, indirettamente, deve necessariamente rispettare i requisiti del Regolamento 2022/2554.

Per il fornitore, tale obbligo quindi non è di tipo normativo (non viene sanzionato se non rispetta tali clausole), ma di tipo contrattuale.

Nei paragrafi precedenti si è inoltre accennato che il Regolamento 2022/2554 ha impatto su un numero veramente elevato di fornitori ICT.

Questa affermazione trova la sua ragione di essere in una particolarità del Regolamento 2022/2554, a dire il vero già presente nella precedente normativa di EBA, ma ulteriormente rafforzata nel nuovo Regolamento.

Il Regolamento 2022/2554 richiede che non solo il fornitore ICT diretto dell'entità finanziaria sia soggetto al completo presidio da parte di quest'ultima, ma tale controllo deve estendersi all'intera catena di fornitura e comprendere quindi tutti i sub fornitori, a qualunque livello della catena questi si posizionino, come meglio specificato nei documenti integrativi al Regolamento dedicati ai fornitori e subfornitori.

Per tale motivo, come rappresentato per i diretti fornitore ICT delle entità finanziarie, che devono adeguarsi ad una serie di requisiti del Regolamento 2022/2554 per obblighi contrattuali, anche i subfornitori subiscono la stessa sorte.

Ne consegue che una qualunque azienda che venda un prodotto ICT o svolga un servizio ICT rientra, potenzialmente, nell'ambito di applicazione del Regolamento 2022/2554.

È infatti sufficiente che un suo cliente faccia parte della catena di fornitura di un'entità finanziaria perché ciò accada e, quindi, anche se non si è fornitori diretti di una entità finanziaria, la probabilità che un'azienda che operi in ambito ICT sia coinvolta dal rispetto del Regolamento è molto alta.

Peraltro, vi è al momento una scarsa consapevolezza da parte delle aziende del settore ICT del loro potenziale coinvolgimento nel rispetto dei requisiti del Regolamento 2022/2554.

Inoltre le entità finanziarie difficilmente riusciranno a ri formalizzare i contratti in essere con i loro diretti fornitori ICT per adeguarli ai requisiti del Regolamento 2022/2554 nei tempi previsti dalla normativa.

Solo dopo questo passaggio i diretti fornitori ICT delle entità finanziarie potranno a loro volta ri formalizzare i contratti con i loro fornitori ICT e così a scendere, lungo tutta la catena di fornitura.

Passeranno quindi mesi, se non anni, affinché si raggiunga una piena conformità che, nel momento della stesura di questo articolo, è anche impossibile da implementare, non essendo ancora disponibile, come già ricordato lato subfornitori, un importante tassello del quadro normativo che regola la gestione della catena di fornitura.

8 – Gli errori ed i limiti di DORA

Il Regolamento 2022/2554 non è esente da limiti ed errori.

Un primo limite è stato più volte evidenziato e riguarda il tipo di approccio che il legislatore ha adottato nella costruzione della normativa che integra il Regolamento 2022/2554.

Ma anche la normativa consolidata non è esente da limiti ed errori.

Analizziamo un caso specifico, quello relativo al rischio di concentrazione.

Con tale termine, come indicato dall'articolo 2 del Regolamento, si intende *l'esposizione a fornitori terzi critici di servizi TIC, singoli o molteplici e correlati tra loro, che crea un grado di dipendenza tale da detti fornitori che l'indisponibilità, i guasti o altri tipi di carenze che si verificassero presso di essi potrebbero mettere a repentaglio la capacità di un'entità*

finanziaria di assolvere funzioni essenziali o importanti oppure di assorbire altri tipi di effetti avversi, comprese perdite cospicue, o potrebbero mettere a repentaglio la stabilità finanziaria dell'intera Unione.

Da tale definizione sembrerebbe che il rischio di concentrazione sia da valutare unicamente per i fornitori critici, ma in tal senso non si esprime l'articolo 29, dal quale appare evidente tale rischio debba essere valutato per tutti i fornitori:

Articolo 29 Valutazione preliminare del rischio di concentrazione delle TIC a livello di entità

1. All'atto dell'identificazione e della valutazione dei rischi di cui all'articolo 28, paragrafo 4, lettera c), le entità finanziarie tengono conto altresì dell'eventualità che la prevista conclusione di un accordo contrattuale relativo a servizi TIC a supporto di funzioni essenziali o importanti possa avere una delle seguenti conseguenze:

…

b) la presenza di molteplici accordi contrattuali relativi alla prestazione di servizi TIC a supporto di funzioni essenziali o importanti con lo stesso fornitore terzo oppure con fornitori terzi strettamente connessi.

Le entità finanziarie vagliano i benefici e i costi di soluzioni alternative, quali il ricorso a diversi fornitori terzi di servizi TIC, verificando se e come le soluzioni previste soddisfino le esigenze commerciali e consentano di conseguire gli obiettivi fissati nella propria strategia di resilienza digitale.

Nell'articolo 29 non vi è infatti il minimo cenno al fatto che i fornitori citati siano solo fornitori critici.

Vi è quindi una discrepanza ed incoerenza fra il contenuto di 2 articoli della normativa in merito allo stesso requisito.

Ma anche la logica di determinazione del rischio di concentrazione non raggiunge lo scopo che il legislatore si era prefissato.

La normativa prevede infatti che debba essere valutato il rischio di concentrazione collegato ad un fornitore ICT, ma tale termine viene utilizzato dal Regolamento 2022/2554 indistintamente sia per i fornitori ICT diretti della entità finanziaria, sia per i subfornitori (si veda al riguardo l'articolo 3 del Regolamento).

In particolare, per quanto attiene i subfornitori, viene valutato il rischio di concentrazione considerando quanti fornitori diretti della entità finanziaria (o sub fornitori) insistano su di essi.

Ed è proprio qui il problema.

Si consideri il fatto che quattro finitori ICT di applicazioni in cloud utilizzino lo stesso fornitore di piattaforme cloud.

Questo subfornitore avrebbe un certo livello di criticità determinato dal fatto che, in sua assenza, i quattro fornitori ICT diretti non potrebbero erogare il loro servizio.

Si consideri ora la presenza di altri dieci fornitori di servizi non ICT che utilizzino lo stesso subfornitore.

Il rischio di concentrazione su quello specifico subfornitore dovrebbe a questo punto sommare quattro (numero di fornitori ICT che utilizzano quel subfornitore), a dieci (numero di fornitori non ICT che utilizzano quel subfornitore), ottenendo un rischio di concentrazione di quattordici.

Ed è qui che la normativa evidenzia il suo grosso limite, in quanto per il Regolamento 2022/2554 il rischio rimane quattro, (si veda al riguardo il **Final Report On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554**), in quanto vengono considerate solo le catene di fornitura che hanno come primo fornitore, un fornitore ICT.

Appare evidente come il rischio reale di concentrazione, in particolare con riferimento all'ambiente cloud, possa essere largamente sottovalutato dal Regolamento 2022/2554, che manca così uno dei suoi obiettivi principale, e cioè il presidio della catena di fornitura.

9 – Conclusioni

Il Regolamento 2022/2554 costituisce sicuramente un importante tappa nel percorso teso ad aumentare il livello di sicurezza e resilienza delle infrastrutture critiche dell'UE, ma necessità ancora di qualche affinamento per poter risultare pienamente efficace e, probabilmente è poco flessibile per potersi adattare in tempi ragionevoli alla evoluzione tecnologica.
Una impostazione della normativa più simile a quella sperimentata con successo per il GDPR sarebbe stata una scelta più appropriata.

10 - Bibliografia

[1] "Regolamento 2022/2554", Parlamento europeo, 2022

[2] "Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022", Banca d'Italia, 2024

[3] "Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario", Senato della Repubblica, 2025

[4] "NIST Cybersecurity Framework 2.0", NIST, 2024

[5] Ross, R. e altri, "Developing Cyber-Resilient Systems", NIST, 2021

[6] Butti, G., "Manuale di resilienza", ITER, 2023

[7] Butti, G., "La gestione dei rischi nella supply chain", ITER, 2025 (in fase di pubblicazione)