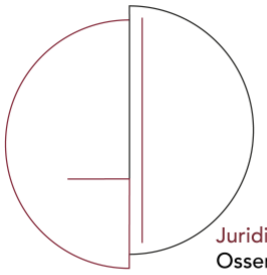

DIRITTO E NUOVE TECNOLOGIE*

Rubrica di aggiornamento dell'OGID.

Questa rubrica di aggiornamento è curata dal Prof. Salvatore Orlando e dal Dott. Daniele Imbruglia nell'ambito delle attività dell'OGID, Osservatorio Giuridico sulla Innovazione Digitale, costituito presso il Dipartimento di Diritto ed Economia delle Attività Produttive dell'Università di Roma "La Sapienza" (https://web.uniroma1.it/deap/ogid - jodi.deap@uniroma1.it).

* Contributo non sottoposto a referaggio ai sensi dell'art. 9, V co., del Regolamento per la classificazione delle riviste nelle aree non bibliometriche, approvato con Delibera del Consiglio Direttivo n. 42 del 20.02.2019.

precedente esercizio finanziario, se constata che il *gatekeeper* ha commesso, in relazione allo stesso servizio di piattaforma di base, un'infrazione identica o simile a una già rilevata con decisione negli otto anni precedenti (art. 30, par. 2 DMA).

Alle sanzioni pecuniarie si accompagna, nei casi di inosservanza sistematica, il potere di adozione, da parte della Commissione, di atti di esecuzione che impongono all'impresa l'assunzione di qualsiasi rimedio comportamentale o strutturale proporzionato e necessario per garantire l'effettivo rispetto del regolamento (art. 18, par. 1 DMA). L'inosservanza si qualifica come sistematica laddove la Commissione abbia adottato negli ultimi otto anni almeno tre decisioni di esecuzione a norma dell'art. 29 DMA in relazione a uno dei suoi servizi di piattaforma di base.

VALENTINO RAVAGNANI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R1925&from=EN

3. Approvato il 'DORA': Regolamento (UE) 2022/2554 del 14.12.2022 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

Nella Gazzetta ufficiale dell'Unione europea del 27.12.2022 è stato pubblicato il Regolamento (UE) 2022/2554 del 14.12.2022 relativo alla resilienza operativa digitale per il settore finanziario (di seguito solo il "**Regolamento**" o "**DORA**", acronimo per *Digital Operational Resilience Act*). Si tratta del testo rispondente al documento P9_TA(2022)0381 del 10 novembre 2022 con il quale il Parlamento europeo approvava, con alcune modifiche frutto di un compromesso col Consiglio, la proposta di regolamento COM(2020)0595.

Il Regolamento si inserisce nel "Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo" elaborato nel 2018 dalla Commissione europea. Il testo finale del DORA si pone in continuità anche col parere congiunto emesso nell'aprile 2019 da EBA, ESMA ed EIOPA (di seguito le Autorità Europee di Vigilanza o "**AEV**") che invocava "*l'adozione di un approccio coerente ai rischi informatici nel settore finanziario e si raccomandava di potenziare, in maniera proporzionata, la resilienza operativa digitale*".

Il settore della finanza è stato fortemente interessato dall'evoluzione dell'*Information and Comunication Technology* (c.d. "**ICT**" o "**TIC**" nell'acronimo italiano) tanto che quest'ultima ha *"conquistato un ruolo essenziale nella fornitura di servizi finanziari*" (Considerando 2) DORA). Soprattutto alla luce di possibili attacchi informatici, è riconosciuto che tale "interconnessione" tra finanza e ICT può rappresentare una criticità del sistema finanziario, particolarmente per quegli enti con un ruolo "sistemico" nel mercato a causa delle loro dimensioni (cfr. Considerando 3) DORA e il riferimento ivi contenuto al Comitato europeo per il rischio sistemico – CERS/ESRB dal suo acronimo in lingua inglese: *European Systemic Risk Board*).

All'evoluzione tecnologica, inoltre, non si è affiancata un'evoluzione normativa che, finora, si mostra frammentata e, sostanzialmente, di livello nazionale. Ecco, dunque, che il Regolamento "*mira a consolidare e aggiornare i requisiti in materia di rischi informatici nell'ambito dei requisiti in materia di rischi operativi che sono stati finora trattati separatamente in vari atti giuridici dell'Unione*" e "*colma pertanto le lacune o pone rimedio alle incoerenze di taluni fra i precedenti atti legislativi* … [nds, Esso] *dovrebbe altresì accrescere la consapevolezza dei rischi informatici e riconoscere che gli incidenti connessi alle TIC e la mancanza di resilienza operativa potrebbero compromettere la solidità delle entità finanziarie*" (Considerando 12) DORA). Il Regolamento si inserisce in un percorso normativo dell'UE dove si colloca anche il Regolamento (UE) 2022/858 relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito (c.d. **Regolamento DLT**) (su cui v. notizia n. 2 nel numero 2/2022 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf) e la proposta di **Regolamento sui mercati delle criptovalute** (c.d. MiCAR, acronimo per *Markets in Crypto-Assets Regulation*), (su cui v. notizia n. 3 nel numero 2/2022 in questa Rubrica: http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf).

I destinatari del DORA, chiamati "entità finanziarie" (art. 2.2 DORA), sono sia soggetti tradizionali (ad esempio, banche e assicurazioni), sia "*fornitori di servizi per le cripto-attività*", sia i "*fornitori terzi di servizi TIC*" (art. 2.1 DORA).

L'art. 3 del Regolamento elenca una serie di definizioni, mentre il successivo art. 4 richiama il principio di proporzionalità, sancito anche nel considerando 13, per cui le norme del DORA dovranno essere applicate *"tenendo conto delle …*

dimensioni e del … profilo di rischio complessivo, nonché della natura, della portata e della complessità dei loro servizi, delle loro attività e della loro operatività".

L'art. 1 descrive l'oggetto del Regolamento che sostanzialmente può dividersi in 5 pilastri, similmente a quanto ipotizzato nella precedente versione del testo, come qui di seguito riassunti.

I. Governance e organizzazione (art. 5 DORA)

Le entità finanziarie devono predisporre "*un quadro di gestione e di controllo interno che garantisca una gestione efficace e prudente di tutti i rischi informatici, … al fine di acquisire un elevato livello di resilienza operativa digitale*" (art. 5). L'organo amministrativo ha "*la responsabilità generale di definire e approvare la strategia di resilienza operativa digitale*" e a tal fine deve: i) predisporre "*politiche miranti a garantire il mantenimento di standard elevati di disponibilità, autenticità, integrità e riservatezza dei dati*"; ii) definire "*chiaramente ruoli e responsabilità per tutte le funzioni connesse alle TIC"* e iii) stabilire *"adeguati meccanismi di governance al fine di garantire una comunicazione, una cooperazione e un coordinamento efficaci e tempestivi*" tra le menzionate funzioni (art. 5). All'organo gestionale compete anche l'approvazione, supervisione e riesame dei piani di risposta e ripristino delle infrastrutture ICT in seguito a attacchi informatici.

Vale la pena precisare che le suddette disposizioni sono coerenti con le Linee guida dell'EBA (EBA/GL/2019/04) sulla sicurezza e gestione del rischio ICT e dell'EIOPA (EIOPA-BoS-20/600) sulla sicurezza e governance ICT.

II. Risk management (artt. 6 – 16 DORA)

L'art. 6 si preoccupa di stabilire che le entità finanziarie istituiscano un quadro per la gestione dei rischi informatici "*solido, esaustivo e adeguatamente documentato*" che comprenda "*almeno*" strategie e procedure per proteggere i dati e per assicurare la resilienza e continuità delle attività ICT (art. 11).

Con la sola eccezione delle microimprese, per cui il Regolamento non stabilisce una tempistica, il quadro per la gestione dei rischi informatici deve essere riesaminato annualmente e, comunque, in occasione di gravi incidenti informatici o su richiesta delle AEV, che possono sempre chiedere informazioni sul quadro generale.

Le entità finanziarie devono costantemente monitorare e aggiornare le proprie strategie di resilienza e infrastrutture digitali, che devono essere proporzionate alle proprie dimensioni, affidabili e resilienti (art. 7 e 9). Come anticipato, alle entità finanziarie spetta anche l'individuazione delle funzioni aziendali che utilizzano strumenti ICT (art. 8), le quali devono costantemente essere sensibilizzate e formate sul rischio informatico. Nondimeno, un numero sufficiente di risorse umane (adeguatamente formato) deve essere dedicato alla raccolta di informazioni sulla vulnerabilità dei sistemi ICT aziendali e le sue possibili conseguenze (art. 13).

In aggiunta a quanto sopra, gli enti finanziari devono predisporre meccanismi idonei ad individuare automaticamente e tempestivamente le attività anomale, nonché "*punti di vulnerabilità (points of failure) importanti*" (art. 10).

Le entità finanziarie devono predisporre in anticipo "*piani di comunicazione delle crisi* [nds, che includano la comunicazione iniziale e gli aggiornamenti sui suoi sviluppi] *che consentano una divulgazione responsabile di informazioni riguardanti, almeno, gravi incidenti connessi alle TIC o vulnerabilità*" ai vari stakeholder (art. 14).

In occasione di incidenti ICT, gli enti finanziari devono esaminarne le cause integrando quanto è stato imparato dal fenomeno nel quadro per la gestione dei rischi informatici.

III. Gestione, classificazione e segnalazione degli incidenti informatici (artt. 17 – 23 DORA)

Con le norme in commento il Regolamento intende semplificare alcuni adempimenti già previsti dalla normativa vigente.

In particolare, le entità finanziarie dovranno predisporre un "*processo di gestione degli incidenti connessi alle TIC*" (art. 17), implementando piani di continuità operativa e di disaster recovery, nonché classificare e segnalare gli incidenti ICT, soprattutto quelli gravi (art. 19), all'Autorità competente. Il Regolamento non prevede scadenze temporali per la segnalazione rimettendo alle AEV l'adozione di standard tecnici entro 18 mesi dall'entrata in vigore della disciplina in commento.

Si rappresenta che le AEV dovranno emanare una relazione congiunta sulla fattibilità di un sistema centralizzato di segnalazione degli incidenti ICT (art. 21).

Il Regolamento, inoltre, all'art. 18, par. 2 stabilisce che le minacce informatiche si definiscono significative "*in base alla criticità dei servizi a rischio, comprese le operazioni dell'entità finanziaria, il numero e/o la rilevanza di clienti o controparti finanziarie interessati e l'estensione geografica delle aree a rischio*". Se, da un lato, la registrazione di tali minacce è obbligatoria, dall'altro, il DORA, coerentemente con quanto stabilito dalla direttiva 2016/1148/UE (c.d. direttiva

NIS), prevede che la notifica alle Autorità nazionali di vigilanza sia volontaria laddove le entità finanziarie "*ritengano che la minaccia sia rilevante per il sistema finanziario, gli utenti dei servizi o i clienti*" (art. 19).

IV. Test di resilienza operativa digitale (artt. 24 – 27 DORA).

Il Regolamento prevede che annualmente gli enti finanziari, diversi dalle microimprese, debbano sottoporre le proprie funzioni e servizi ICT critici e il proprio quadro di gestione dei rischi informatici a un test di resilienza operativa digitale "*solido ed esaustivo*" al fine di individuare le criticità dei propri sistemi e risolverle (art. 24).

In aggiunta a quanto sopra, le entità finanziare di rilevanti dimensioni, o che hanno un ruolo sistemico nel mercato finanziario, dovranno svolgere anche "*test di penetrazione basati su minacce, con cadenza almeno triennale*", c.d. *Thread-Led Penetration Testing* o TLPT (art. 26). Tali test devono riguardare almeno le funzioni e i servizi critici (art. 24).

I test devono essere svolti da soggetti, interni o esterni – quest'ultimi certificati dalle Autorità nazionali competenti -, indipendenti e con elevate competenze tecniche. In particolare, quelli incaricati di svolgere i test di penetrazione devono avere i requisiti di cui all'art. 27. Se i test sono svolti da un soggetto interno, le entità finanziarie dovranno dedicare risorse sufficienti a tale attività e garantiscono che siano evitati conflitti d'interessi durante le fasi di progettazione ed esecuzione del test. I test, inoltre, devono essere sempre improntati al principio di proporzionalità informante il Regolamento.

V. Gestione dei rischi informatici derivanti da terzi (artt. 28 – 44 DORA)

Il DORA dedica attenzione anche ai fornitori di servizi ICT critici i quali corrono i medesimi rischi delle entità finanziarie. Essi, pertanto, saranno assoggettati ad ampi poteri di supervisione e vigilanza delle AEV. Così quest'ultime potranno chiedergli di apportare modifiche alle proprie misure di sicurezza. Nondimeno, laddove ricorrano i requisiti stabiliti nel Regolamento, le AEV potranno imporre alle entità finanziarie di sospendere o risolvere i contratti con i propri fornitori di servizi ICT.

La normativa prevede anche delle condizioni contrattuali minime che gli operatori finanziari dovranno includere nei propri contratti con fornitori di servizi ICT al fine di garantire il rispetto delle previsioni del DORA.

Per quanto qui rileva, infine, bisogna precisare che il Regolamento rimette alla normativa secondaria, ossia i *Regulatory Technical Standard* o gli *Implementing Technical Standard*, da adottare a seconda dei casi entro 12 o 18 mesi dall'entrata in vigore del Regolamento, la regolazione di aspetti di dettagli del Regolamento stesso. Peraltro, la violazione delle disposizioni del DORA è sanzionabile dalle Autorità Europee di Vigilanza (artt. 50 ss. DORA).

L'art. 64 prevede che il Regolamento entri in vigore il ventesimo giorno successivo alla sua pubblicazione nella Gazzetta ufficiale dell'Unione europea e che si applichi a decorrere dal 17 gennaio 2023.

EMANUELE STABILE

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2554&from=EN

4. Le modifiche apportate alla disciplina dell'abuso di dipendenza economica di cui alla legge sulla subfornitura, con decorrenza dal 31 ottobre 2022

Con decorrenza dal 31 ottobre 2022, l'art. 33 della legge 5 agosto 2022, n. 118 ha modificato la disciplina dell'abuso di dipendenza economica contenuta nella legge sulla subfornitura (art. 9 della legge 18 giugno 1998, n. 192 recante la disciplina della subfornitura nelle attività produttive: di seguito "**l. subfornitura**"), disponendo due integrazioni di diritto sostanziale riguardanti le piattaforme digitali, e una modifica generale (ossia non limitata ai rapporti riguardanti le piattaforme digitali) sulla competenza giurisdizionale.

La prima integrazione riguarda la nozione di dipendenza economica. Come noto, la dipendenza economica non è di per sé vietata dalla l. subfornitura, essendone invece vietato l'abuso. Interessante appare la formulazione della norma che richiede di guardare agli "effetti di rete" e alla "disponibilità dei dati" per stabilire se possa dirsi che una piattaforma digitale abbia o meno un "ruolo determinante per raggiungere utenti finali o fornitori" dell'impresa di cui importi predicare una situazione di dipendenza economica dalla medesima piattaforma digitale. La seconda integrazione riguarda per l'appunto l'abuso di dipendenza economica. La norma prevede come figure sintomatiche di abuso di dipendenza economica pratiche informative ingannevoli (commissive od omissive) relativamente al servizio erogato dalla piattaforma digitale, oppure pratiche della piattaforma digitale che consistono nel pretendere dall'impresa prestazioni ingiustificate ovvero