BonelliErede

Practice* Concorrenza/*Antitrust

***Practice* Diritto dell'Unione europea**

16 Febbraio 2026

Cybersecurity Act 2: le nuove regole europee in materia di *supply chain*, certificazioni e fornitori "ad alto rischio"

Autori

Claudio Tesauro
Claudio.Tesauro@belex.com
Tel. +39 06 845511

Sara Lembo
Sara.Lembo@belex.com
Tel. +39 06 845511

Pier Paolo Moroni
Pier.Moroni@belex.com
Tel. +39 06 845511

1. Introduzione

In un contesto caratterizzato da una rapida e costante evoluzione tecnologica, la tutela della cybersicurezza e la gestione dei rischi legati alla catena di approvvigionamento dei componenti ICT sono da qualche anno al centro della strategia digitale europea. Le infrastrutture e i servizi (*e.g.* reti, *cloud*, *data center*, *software*) sono, infatti, sempre più esposti a rischi derivanti non solo da vulnerabilità tecniche ma anche da fattori legati al contesto geopolitico in cui operano i fornitori.

In questo scenario, il 20 gennaio 2026, la Commissione europea ("**Commissione**") ha pubblicato una proposta di regolamento (c.d. "**Cybersecurity Act 2**" o "**CSA2**") che mira a rafforzare e armonizzare i presidi di sicurezza informatica e a semplificare gli oneri di *compliance* per le imprese attive negli Stati membri.[1]

La nuova proposta, che si inserisce in un percorso avviato nel 2019, ha l'obiettivo di creare un quadro europeo più strutturato per la gestione dei rischi di filiera e consolidare il sistema delle certificazioni in modo da non rendere necessari ulteriori adempimenti di conformità.

2. Le origini del CSA2: l'approccio UE dal 2019 ad oggi

Il percorso europeo in materia di cybersicurezza ha avuto inizio nel 2019 con il Regolamento (UE) 2019/881 (*Cybersecurity Act*) che, da un lato, ha attribuito all'Agenzia europea per la sicurezza informatica ("**ENISA**") un mandato permanente e un ruolo centrale di supporto tecnico-operativo alle istituzioni UE e, dall'altro, ha istituito **sistemi volontari** di

[1] Il CSA2 fa parte di un pacchetto di misure più ampio e strettamente collegato alla parallela proposta di direttiva che modifica la Direttiva (EU) 2022/2555 (*Direttiva NIS2*).

certificazione per prodotti, servizi e processi ICT al fine di favorire *standard* di sicurezza più omogenei nel mercato interno.[2]

Questo impianto normativo si è poi rafforzato nel tempo attraverso **iniziative settoriali** che hanno accelerato l'implementazione della disciplina di riferimento negli Stati membri**.**

Nel settore delle telecomunicazioni, ad esempio, la Commissione ha chiarito con la Raccomandazione (UE) 2019/534 che la valutazione dei rischi deve includere non solo i profili tecnici (*i.e.* vulnerabilità dei *software*, malfunzionamenti, complessità delle architetture) ma anche fattori legati al quadro giuridico e politico del Paese in cui opera il fornitore e, più in generale, al rischio di ingerenze di Stati extra-UE.

Le considerazioni espresse nella Raccomandazione sono state poi cristallizzate nel Rapporto coordinato sulla sicurezza delle reti 5G[3] e, nel 2020, nel c.d. UE 5G Toolbox, un pacchetto di misure strategiche che ha legittimato – in una logica dichiaratamente *risk-based* – strumenti di mitigazione quali la **diversificazione** dei fornitori e la possibilità di **restrizioni o esclusioni** nei confronti di quelli "*ad alto rischio*".[4]

Nel 2023, la Commissione ha completato il quadro normativo in materia di gestione del rischio ICT attraverso:

- la Direttiva 2022/2555 ("**Direttiva NIS2**")[5] che, oltre ad individuare l'elenco specifico dei destinatari delle disposizioni ("**Soggetti NIS**"), estende gli obblighi di cybersicurezza a una serie di altri settori definiti come "*altamente critici*", includendovi le infrastrutture digitali, la fornitura di servizi ICT e la pubblica amministrazione;
- il Regolamento (UE) 2022/2554 ("**Regolamento DORA**"), focalizzato sul settore finanziario, che impone una *governance* strutturata del rischio attraverso strategie volte a diversificare i fornitori e stipulare accordi soltanto a condizione che gli stessi soddisfino adeguati *standard* di sicurezza.

---

[2] Si fa riferimento allo *European Cybersecurity Certification Framework* ("**ECCF**").

[3] Il rapporto contiene la sintesi delle valutazioni degli Stati membri sui profili di rischio delle reti 5G. Nello specifico, le principali sfide individuate riguardano l'innovazione dei *software* e il ruolo dei fornitori nella costruzione e nella gestione delle reti 5G. Si rilevano inoltre rischi connessi alla maggiore esposizione ad attacchi esterni, legata al moltiplicarsi di potenziali punti di accesso (*i.e.* possibili falle nei *software* dei fornitori). Secondo il rapporto, queste sfide creano un nuovo paradigma di sicurezza, rendendo necessario per gli Stati membri adottare le misure di mitigazione necessarie.

[4] La Commissione ha monitorato nel tempo l'attuazione del *Toolbox* rimarcando, con la Comunicazione del 15 giugno 2023, il tema della persistente dipendenza da fornitori ad alto rischio e la necessità di decisioni più omogenee e incisive tra Stati membri.

[5] La Direttiva NIS2 sostituisce la precedente Direttiva 2016/1148 (cd. NIS1).

3. La nuova proposta CSA2: gli ambiti di intervento

Alla luce del quadro appena delineato, il Cybersecurity Act 2 mira a superare i limiti di un impianto "volontario" e frammentato, attraverso un **approccio più operativo che si concentra su quattro direttrici.**

(i) ***Supply chain* ICT e gestione dei fornitori**: la proposta introduce un *trusted ICT supply chain framework* a livello UE, permettendo alla Commissione di designare fornitori ad alto rischio e di imporre divieti e/o misure di mitigazione mirate.[6] Nel settore delle telecomunicazioni, la proposta si collega alla logica di "*de-risking*" delle reti mobili europee e prevede l'obbligo a carico degli operatori di rimuovere dai propri *asset* i componenti ICT di fornitori extra-UE secondo modalità che saranno definite con provvedimenti *ad hoc*.[7]

(ii) **Sistemi di certificazione**: il CSA2 rende il sistema di certificazione europea più rapido ed efficace, prevedendone l'utilizzo per dimostrare la conformità ai requisiti di sicurezza, evitando dunque alle aziende ulteriori oneri di *compliance*. [8]

(iii) **Semplificazione del quadro normativo:** la riforma riduce gli oneri amministrativi e di vigilanza anche per le autorità competenti, favorendo una maggiore coerenza nell'attuazione delle normative *cyber*, quali NIS2 e DORA.

(iv) **Rafforzamento del ruolo operativo di ENISA**: il pacchetto rende più incisive alcune funzioni operative di ENISA che, tra le altre cose, potrà fornire orientamenti mirati agli Stati membri e alla Commissione in materia di gestione dei rischi di sicurezza informatica, contribuire a svolgere valutazioni coordinate a livello UE e sviluppare sistemi volti ad attestare il possesso dei requisiti previsti dalle normative di riferimento.

---

[6] Le restrizioni si applicheranno a seguito di una valutazione formale, avviata dalla Commissione o da almeno tre Stati membri e fondata su analisi di mercato e studi di impatto condotti nell'ambito del nuovo *trusted ICT supply chain framework*. Qualora un paese terzo presenti "*serious and structural non-technical risk to ICT supply chains*", ai fini della successiva designazione "*as a country posing cybersecurity concerns*", la Commissione dovrà condurre una valutazione basata su (i) l'esistenza, nel Paese terzo, di leggi/pratiche che obbligano le aziende a comunicare alle autorità vulnerabilità *software/hardware* prima che risultino note; (ii) l'assenza di rimedi giudiziari che possano correggere le preoccupazioni di sicurezza; (iii) la presenza di *cyber*-attacchi riconducibili al Paese terzo, uniti alla sua scarsa volontà o capacità di cooperare con UE o Stati membri. Le violazioni delle misure di mitigazione possono comportare sanzioni fino al 7% del fatturato annuo globale.

[7] Per le reti mobili il *phase-out* è previsto entro 36 mesi dalla pubblicazione dell'elenco dei fornitori ad alto rischio. Per reti fisse e satellitari verranno previste ulteriori tempistiche.

[8] Le certificazioni si continuano ad applicare a prodotti e servizi ICT e si estendono alla valutazione della posizione complessiva dell'azienda in materia di sicurezza informatica.

La proposta seguirà la procedura legislativa ordinaria, che dovrebbe concludersi entro un paio di anni. Una volta adottato, il Regolamento sarà direttamente applicabile in tutti gli Stati membri.

In tale scenario, sarà importante che le misure siano **proporzionate** e definite sulla base di **criteri oggettivi**: un'eccessiva compressione della concorrenza – attraverso l'esclusione automatica di fornitori extra europei – potrebbe tradursi in aumento dei costi, rallentamento degli investimenti e minore innovazione, senza produrre necessariamente benefici equivalenti in termini di sicurezza.

4. Il *focus* sull'Italia: l'adeguamento all'assetto europeo e le procedure competitive

In Italia, l'assetto normativo europeo si riflette sia negli **strumenti di cybersicurezza** sia nelle **procedure competitive** in cui l'adeguatezza delle offerte viene valutata non solo alla luce di elementi tecnici ma anche di requisiti strategico-regolamentari degli operatori coinvolti.

Sul primo versante, dopo il recepimento della Direttiva NIS2 (d.lgs. 138/24), molti operatori sono oggi tenuti ad adottare precise misure tecniche e organizzative. In concreto, i c.d. Soggetti NIS (*i.e.* operatori essenziali in settori critici e altamente critici individuati dalla normativa) devono registrarsi su una piattaforma digitale dell'Agenzia Nazionale per la Cybersicurezza ("**ACN**") e adottare un *set* di misure di gestione del rischio, incluse apposite garanzie rispetto alla propria catena di approvvigionamento.[9]

In parallelo, la disciplina nazionale prevede che la pubblica amministrazione può acquistare solo servizi *cloud* di fornitori inclusi in uno specifico catalogo tenuto dall'ACN con implicazioni concrete per la strategia di accesso al mercato pubblico. [10]

Sul versante delle procedure competitive, particolarmente rilevante è l'introduzione di un **meccanismo di premialità** collegato alla provenienza delle tecnologie per la partecipazione alle gare per la fornitura di beni e servizi ICT.

---

[9] Le misure di sicurezza adottate dai Soggetti NIS sono oggetto di valutazione da parte dell'ACN, che ne verifica la conformità con cadenza annuale e che può "*imporre specifici obblighi proporzionati e graduali ai soggetti […] che forniscono servizi, anche digitali, alla pubblica amministrazione*". Per maggiori informazioni sulle novità introdotte dalla Direttiva NIS2 in merito agli obblighi di registrazione presso l'ACN, ai relativi adempimenti in capo ai Soggetti NIS e alle responsabilità degli organi di gestione delle imprese in materia di cybersicurezza si veda la precedente Newsletter del Focus Team Innovazione e Trasformazione digitale.

[10] Cfr. Decreto direttoriale, n. 29 del 2 gennaio 2023.

Il DPCM 30 aprile 2025, come modificato dal DPCM 2 ottobre 2025, ha infatti previsto che i bandi devono assegnare un **punteggio premiale** per tecnologie provenienti da **Italia/UE/NATO**,[11] sulla base di un'analisi del BOM (*Bill of Materials*), ossia una lista dettagliata delle componenti del bene/servizio ICT e del loro produttore.

Le Linee Guida per l'applicazione dei criteri di premialità dell'ACN chiariscono le modalità applicative, distinguendo tra (i) **telecomunicazioni** (*i.e.* 4G/5G), per cui il massimo punteggio è attribuibile in modo frazionato in funzione della provenienza dei macro-componenti di rete (RAN, *backhoul* e *core network*); e (ii) **beni e servizi ICT**, per cui i criteri di premialità sono soggetti a un meccanismo "*on/off*", con assegnazione del punteggio pieno (non frazionabile) solo se tutti i componenti e servizi di livello 1 della BOM rispettano i requisiti di provenienza dai paesi individuati dal DPCM.

Pur essendo costruiti come "premialità" e non come divieti espliciti, questi strumenti possono avere un **effetto significativo sulla concorrenza**, soprattutto nelle gare dove il punteggio tecnico ha un peso importante nell'assegnazione della commessa, orientando gli operatori verso fornitori ritenuti affidabili per ragioni strategiche ma che non necessariamente sono i migliori in termini di qualità, innovazione, sicurezza tecnica e prezzi.

4. Conclusioni

Il pacchetto di proposte presentato dalla Commissione rappresenta un passo decisivo verso la costruzione di un'Europa digitalmente sviluppata e strategicamente autonoma, confermando una tendenza ormai chiara: la resilienza digitale non è più solo un tema tecnico, ma è un fattore che incide su accesso al mercato, relazioni contrattuali, procedure di gara e, in ultima analisi, sulla capacità di competere su scala globale.

Sarà tuttavia necessario garantire un equilibrio tra sicurezza e tutela della concorrenza: misure basate su criteri chiari, verificabili e proporzionati possono rafforzare la resilienza digitale senza ridurre l'effettiva contendibilità dei mercati e/o generare posizioni di privilegio a cui non corrispondo effettivi meriti in termini di qualità, innovazione, sicurezza tecnica e prezzi.

Per le imprese la sfida sarà cogliere le opportunità offerte dal nuovo *framework*, preparandosi ad affrontare un panorama regolatorio in cui l'attenzione alla sicurezza informatica è una condizione strutturale per operare in un mercato sempre più interconnesso e competitivo.

---

[11] Cfr. art. 4, comma 2, DPCM 30 Aprile 2025.

Practice Concorrenza/Antitrust e _Practice_ Diritto dell'Unione Europea

Francesco Anglani

Maurizio Pappalardo

Sara Lembo

Claudio Tesauro

Massimo Merola