In attesa del Cyber Resilience Act. Le opzioni all'esame della Commissione a valle della consultazione pubblica

28/06/2022

DIRITTO EUROPEO E DELLA CONCORRENZA; PROTEZIONE DEI DATI E CYBERSECURITY; COMPLIANCE; RESPONSABILITÀ DA PRODOTTO E SICUREZZA

Roberto A. Jacchia
Andrea Palumbo

In data 25 maggio 2022, la Commissione Europea ha concluso la propria consultazione pubblica sul nuovo atto legislativo sulla "ciberresilienza"[1], ovvero un nuovo regolamento che detti requisiti orizzontali di cibersicurezza dei prodotti digitali e dei servizi accessori. Sulla base dei risultati della consultazione, la Commissione sta lavorando alla stesura del nuovo regolamento.

Con la consultazione pubblica, la Commissione ha inteso raccogliere le opinioni delle parti interessate su come dovrebbe essere affrontata la sfida della cibersicurezza nei c.d. ambienti connessi. In particolare, la Commissione aveva rilevato che un incidente di cibersicurezza che di per sé interessa un solo prodotto può comportare ripercussioni su più prodotti, su un'intera organizzazione o su un'intera catena di approvvigionamento. In tali ipotesi, le attività economiche e sociali possono essere gravemente perturbate, finanche con rischi estremi quando certe infrastrutture altamente sensibili formino oggetto di attacchi informatici (si pensi agli ambienti connessi in ambito sanitario).

Con il nuovo intervento si intende prevalentemente colmare due lacune dell'attuale quadro normativo. In primo luogo, l'attuale disciplina comunitaria si rivolge soltanto ad alcuni aspetti legati alla cibersicurezza dei prodotti digitali tangibili, e se del caso, del software incorporato in essi. Tuttavia, non sono al momento previsti requisiti specifici di cibersicurezza che riguardano l'intero ciclo di vita di un prodotto. Essi sono, invece, essenziali, nel caso di prodotti digitali e servizi accessori, ad esempio, perché un software deve essere costantemente aggiornato. In secondo luogo, la normativa vigente non disciplina tutti i tipi di prodotti digitali. In particolare, da essa sono esclusi alcuni hardware ampiamente utilizzati (ad esempio l'hardware che non rientra nella direttiva

[1] Per maggiori informazioni sulla consultazione pubblica, si veda il seguente LINK.

sulle apparecchiature radio[2] o nel regolamento sui dispositivi medici[3]) e i prodotti software non incorporati, sebbene anche questi prodotti siano sempre più spesso impiegati come veicoli di penetrazione della cibersicurezza.

La consultazione ha consentito alla Commissione di acquisire le informazioni necessarie alla scelta delle opzioni strategiche per colmare le lacune sopra indicate. Al momento dell'apertura della consultazione, erano sul tavolo cinque diverse opzioni.

Due di queste opzioni contemplano gli interventi meno invasivi, consistenti nel mantenimento dello *status quo* oppure nell'utilizzo di strumenti non vincolanti, come orientamenti, raccomandazioni e sistemi di certificazione volontaria. Le altre tre opzioni prevedono invece le diverse forme che l'atto legislativo potrebbe rivestire, e gli strumenti non vincolanti che potrebbero accompagnarlo.

Con la terza opzione, la Commissione considera un intervento normativo *ad hoc* in materia di cibersicurezza dei prodotti digitali e dei servizi accessori. Si limiterebbe ad integrare e modificare i requisiti di cibersicurezza della legislazione vigente, e a regolamentare i nuovi rischi emergenti.

La quarta opzione contempla un approccio misto, con l'adozione di misure vincolanti e non vincolanti. Le misure vincolanti consisterebbero in un intervento normativo orizzontale volto ad introdurre requisiti di cibersicurezza per alcuni prodotti digitali tangibili e servizi accessori. In tale contesto, la Commissione sta considerando due diverse sub-opzioni per la procedura di valutazione della conformità: i) un'autovalutazione della conformità prestabilita, lasciando ai fornitori la scelta di compierla autonomamente o di optare per una valutazione da parte di terzi, ii) prescrivere che l'autovalutazione della conformità sia effettuata da terzi per talune categorie di prodotti, seguendo un approccio basato sul rischio che tenga conto di fattori come l'uso previsto, la funzionalità o la natura del danno potenziale. Le misure non vincolanti, quali orientamenti o raccomandazioni, sarebbero previste solo per i software non incorporati, e solo in una prima fase, riservandosi la possibilità, sulla base dell'impatto delle misure non vincolanti, di proporre in futuro l'adozione di norme vincolanti per i software non incorporati.

Infine, la quinta opzione sarebbe la più invasiva, in quanto richiederebbe un pervasivo intervento normativo, non accompagnato da strumenti non vincolanti. In particolare, la Commissione proporrebbe una normativa orizzontale, che introdurrebbe requisiti espressi di cibersicurezza per numerosi prodotti digitali tangibili ed intangibili e per i servizi accessori associati, ivi inclusi i software non incorporati.

La Commissione ritiene che un intervento normativo con requisiti orizzontali per i prodotti digitali e i servizi accessori avrebbe un'incidenza economica positiva nell'Unione, migliorando i livelli di cibersicurezza, aumentando la fiducia del pubblico nell'economia digitale, diminuendo la perdita di introiti causata da attacchi informatici, e riducendo le ingenti spese associate alla mitigazione specifica delle minacce informatiche.

Queste considerazioni costituiscono solamente la base dell'analisi preliminare, e dovranno essere confermate da un'accurata valutazione d'impatto. Tuttavia, sulla scorta delle valutazioni sin d'ora svolte, la

[2] Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE, GUUE L 153 del 22.05.2014.
[3] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio, GUUE L 117 del 05.05.2017.

Commissione sembra propensa ad adottare nuove norme vincolanti, il che rende improbabile che vengano perseguite la prima o la seconda opzione tra le cinque considerate. In particolare, questa conclusione è corroborata dalle risultanze di uno studio esplorativo[4] già condotto nel 2021 su incarico della Commissione, ove si affermava che l'introduzione di requisiti orizzontali di cibersicurezza per i prodotti digitali costituisce l'opzione migliore in termini di costi e benefici. Per il momento, la Commissione sembra muoversi in questa direzione, salvo che le evidenze e i dati forniti con la consultazione pubblica abbiano provato il contrario.

L'adozione delle nuove misure è prevista entro settembre 2022. La base giuridica dell'intervento normativo sarebbe l'articolo 114 del Trattato sul Funzionamento dell'Unione Europea, che prevede l'applicazione della procedura legislativa ordinaria. Ciò implica che, prima dell'adozione definitiva dell'atto legislativo trascorrerà, con ogni probabilità, un esteso lasso di tempo.

[4] Si veda il report "*Study on the need of Cybersecurity requirements for ICT products – No. 2020-0715*", pubblicato a dicembre 2021, disponibile al seguente LINK.

Roberto A. Jacchia

PARTNER

r.jacchia@dejalex.com

+39 02 72554.1

Via San Paolo 7
20121 - Milano

Andrea Palumbo

ASSOCIATE

a.palumbo@dejalex.com

+32 (0)26455670

Chaussée de La Hulpe 187
1170 - Bruxelles

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com