La Commissione Europea svela la proposta per il Cyber Resilience Act

07/10/2022 DIRITTO EUROPEO E DELLA CONCORRENZA, IT&TMT, PROSPETTIVE

Andrea Palumbo

In data 15 settembre 2022, la Commissione europea ha presentato una nuova proposta legislativa per il Regolamento sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (c.d. «*Cyber Resilience Act*»)[1].

Il *Cyber Resilience Act* rappresenta un'importante novità per la normativa europea sui servizi digitali: per la prima volta sono introdotte norme comuni sulla cibersicurezza per i produttori e gli sviluppatori di prodotti con elementi digitali, sia hardware che software. La Commissione aveva ritenuto opportuno intervenire alla luce del crescente numero di attacchi informatici, che nel 2021 hanno creato danni pari a 5,5 bilioni di euro, e dopo aver osservato che molti dei prodotti con elementi digitali immessi nel mercato sono vulnerabili a tali attacchi.

Il Regolamento si propone di realizzare due principali obiettivi. In primo luogo, si intende incrementare la cibersicurezza dei prodotti con elementi digitali, imponendo che tali prodotti siano prodotti ed immessi nel mercato con un adeguato livello di protezione contro gli attacchi informatici. In secondo luogo, il Regolamento mira a fornire ad utenti e consumatori informazioni sul livello di cibersicurezza dei prodotti che utilizzano, così da permettergli di effettuare scelte consapevoli. Al contempo, l'introduzione di norme comuni europee permetterà di avere un coerente quadro normativo sui requisiti di cibersicurezza, con conseguente facilitazione delle attività di *compliance* di produttori e venditori.

Ecco le principali novità della proposta legislativa.

Per quanto riguarda l'ambito di applicazione, quest'ultimo copre prodotti con elementi digitali per il cui utilizzo è

[1] Il testo del Regolamento è attualmente disponibile solo in lingua inglese: *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020,* COM/2022/454 final del 15.09.2022.

prevista una connessione diretta o indiretta di dati ad un altro dispositivo o alla rete fissa o mobile. Ai sensi del Regolamento, per prodotti con elementi digitali si intendono tutti i prodotti software e hardware e le loro soluzioni remote di trattamento dei dati, inclusi i loro componenti software e hardware che sono immessi nel mercato separatamente. Sono previste tuttavia delle eccezioni, ed il Regolamento non si applica ai prodotti con elementi digitali per cui trovano già applicazione le norme europee sui dispositivi medici e sui veicoli a motore[2]. Inoltre, ne è esclusa l'applicazione anche per i prodotti con elementi digitali già certificati in conformità alle norme europee sull'aviazione civile[3]. Queste eccezioni sono giustificate dal fatto che i prodotti esenti sono già sottoposti ad altri requisiti di sicurezza informatica.

Per quanto riguarda i requisiti di cibersicurezza, il Regolamento prevede che i prodotti con elementi digitali possono essere messi in commercio solo se, da un lato, rispettano i requisiti essenziali di sicurezza elencati nella prima sezione dell'Allegato I al Regolamento e, dall'altro, i processi seguiti per la loro fabbricazione sono conformi ai requisiti essenziali contenuti nella seconda sezione dell'Allegato I. Pertanto, il Regolamento richiede non solo che i prodotti rispettino determinate caratteristiche tecniche, ma anche che i relativi processi di fabbricazione si svolgano con modalità tali da permettere di identificare con precisione le vulnerabilità dei prodotti e le soluzioni tecniche da implementare per attenuarle.

Norme parzialmente differenti sono previste per i prodotti con elementi digitali definiti «critici», elencati nell'Allegato III al Regolamento. Questi prodotti sono stati identificati come critici sulla base dei più alti rischi di cibersicurezza che presentano, e sono suddivisi in due classi, con la seconda classe contenente i prodotti a maggior rischio. La differenza di disciplina, tra i prodotti critici e gli altri prodotti disciplinati dal Regolamento, risiede nelle modalità con cui il produttore deve certificare la loro conformità ai requisiti di cibersicurezza del Regolamento. Per i prodotti non critici è sufficiente un'autovalutazione svolta dal produttore stesso. Per i prodotti critici, dipende dalla loro classe di appartenenza. Per i prodotti di classe I, se la conformità non è dimostrata con standard armonizzati, specificazioni comuni o schemi di certificazione europei, la valutazione di conformità deve essere svolta da una parte terza. Per i prodotti di classe II, è sempre prevista la valutazione di conformità di una parte terza[4]. La lista dell'Allegato III potrà essere modificata nel tempo dalla Commissione europea, tramite atti delegati, qualora ciò sia giustificato dall'evoluzione dei rischi di cibersicurezza dei prodotti o dall'innovazione tecnologica.

Per quanto riguarda gli obblighi informativi, i produttori devono assicurare che i prodotti siano sempre accompagnati dalle informazioni di cui all'Allegato II al Regolamento. La lista dell'Allegato II contiene informazioni sul produttore, sulle caratteristiche tecniche dei prodotti, sugli specifici rischi di cibersicurezza legati ai prodotti, e sull'assistenza tecnica offerta dal produttore in relazione alla sicurezza dei prodotti. Queste informazioni devono essere fornite in un linguaggio chiaro e

[2] In particolare, sono esclusi dall'ambito di applicazione i prodotti a cui si applicano il Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio del 5 aprile 2017 relativo ai dispositivi medici, il Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio del 5 aprile 2017 relativo ai dispositivi medico-diagnostici in vitro, ed il Regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio del 27 novembre 2019 relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada.

[3] In particolare, certificati ai sensi del Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio del 4 luglio 2018 recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea.

[4] Le procedure disponibili sono descritte nell'Allegato VI del Regolamento.

facilmente comprensibile per gli utenti. Gli stessi obblighi informativi sono previsti per gli importatori di prodotti con elementi digitali a cui è apposto il nome o il marchio di una persona fisica o giuridica stabilita fuori dall'Unione.

Un'altra importante novità riguarda la segnalazione all'Agenzia dell'Unione europea per la cibersicurezza (ENISA) di incidenti con i prodotti. Il Regolamento richiede ai produttori di notificare ad ENISA eventuali attacchi informatici, o altri incidenti che possano avere un impatto per la sicurezza informatica del prodotto, entro un termine di 24 ore dal momento in cui ne sono venuti a conoscenza. La notifica deve anche indicare i provvedimenti intrapresi per mitigare i rischi posti dall'incidente.

Gli Stati membri dovranno designare autorità nazionali per la sorveglianza del mercato, che saranno responsabili per l'attuazione del Regolamento. Nei casi di mancata osservanza del Regolamento, le autorità nazionali potranno imporre agli operatori di prendere provvedimenti per rimediare alla violazione, proibire o limitare il commercio di un prodotto, o ordinare che il prodotto sia ritirato dal mercato. Alle autorità nazionali sono anche attribuiti poteri sanzionatori. Il Regolamento fissa i limiti massimi per le sanzioni imponibili, mentre l'ammontare preciso deve essere definito dal diritto nazionale.

Il *Cyber Resilience Act* introdurrà, se approvato, un nuovo corpo di norme a cui dovranno conformarsi gli operatori del mercato. Non si tratta di un'iniziativa isolata, ma ben coordinata con le altre proposte legislative della Commissione sulla sicurezza dei sistemi informatici[5], con cui condivide un approccio basato sul rischio. A tal riguardo, il nuovo Regolamento è stato lodato per il suo approccio rispettoso del principio di proporzionalità, che distingue tra prodotti con bassi ed alti rischi di cibersicurezza.

Per quanto riguarda i prossimi passi, la proposta sarà esaminata dal Parlamento europeo e dal Consiglio, e resta da vedere se saranno apportate significative modifiche.

[5] Tra cui la Direttiva NIS2, ed i c.d. "Cybersecurity Act" e "AI Act".

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