LOGO
Amministrazione
con competenza
prevalente

Relazione
ai sensi dell'art. 6, comma 4, della legge n. 234/2012

Oggetto dell'atto:
Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020

- **Codice della proposta:** COM(2022) 454 final del 16/09/2022
- **Codice interistituzionale:** 2022/0272(COD)
- **Amministrazione con competenza prevalente:** Presidenza del Consiglio dei ministri e Agenzia per la cybersicurezza nazionale

***

Premessa: finalità e contesto

Il Regolamento ha il fine di armonizzare i requisiti di cybersicurezza per i prodotti con elementi digitali in tutti gli Stati membri e rimuovere gli ostacoli alla libera circolazione delle merci. A tal fine sono stati individuate quattro obiettivi specifici:

1. garantire che i fabbricanti migliorino la sicurezza dei prodotti con elementi digitali fin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita;
2. garantire un quadro coerente in materia di cybersicurezza, facilitando la conformità per i produttori di hardware e software;
3. migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali;
4. consentire alle imprese e ai consumatori di utilizzarli in modo sicuro.

La proposta trae le basi dalla Strategia dell'Unione europea per la cybersicurezza per il decennio digitale, adottata dalla Commissione nel dicembre del 2020, che evidenzia come sia fondamentale garantire che i componenti hardware e software, prodotti nell'UE e nei paesi terzi, usati da servizi e infrastrutture critiche e dai dispositivi mobili, siano affidabili, sicuri e garantiscano la protezione dei dati personali. Per addivenire a un mercato unico dei prodotti ICT sicuro è quindi necessario che tutti, nella catena di approvvigionamento (produttori, sviluppatori di software, fornitori di servizi della società dell'informazione) facciano della cybersicurezza una priorità. Sono, inoltre, necessari adeguati requisiti, che devono essere rispettati lungo tutta la catena di approvvigionamento dei prodotti ICT utilizzati in Europa.

Successivamente, tali concetti sono poi stati a più riprese ribaditi e confermati, come, ad esempio, dalle Conclusioni del Consiglio del 23 maggio 2022 sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, le quali invitano la Commissione a proporre, entro la fine del 2022, requisiti comuni in materia di cybersicurezza per i dispositivi connessi.
La proposta si pone quindi come un elemento complementare alla regolamentazione europea in materia di cybersicurezza. Lo strumento legislativo primario dell'UE al riguardo è rappresentato dalla Direttiva (UE) 2016/1148 (cd. Direttiva NIS) sulla sicurezza delle reti e dei sistemi informativi – recepita nell'ordinamento nazionale con il D.Lgs. 65/2018 – la quale impone misure di sicurezza sugli operatori dei settori più critici, ma non contempla, tuttavia, requisiti di sicurezza per i prodotti ICT. Tale impianto è attualmente in corso di revisione, con la proposta di una nuova Direttiva (cd. Direttiva NIS 2) che innalza ulteriormente il livello di ambizione con riguardo all'ambito di applicazione, ai requisiti di sicurezza, nonché ai poteri di vigilanza delle autorità competenti. A queste direttive si aggiungono il Regolamento (UE) 2019/881 (cd. EU Cybersecurity Act – CSA) – il quale definisce il mandato dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA), e

istituisce un quadro europeo per la certificazione della cybersicurezza di prodotti, servizi e processi ICT – e il Regolamento (UE) 2021/887 – che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, nonché la rete dei centri nazionali di coordinamento.

Con riferimento alle iniziative nazionali, ciò appare in linea e a supporto di quanto previsto:

- dalla Strategia di Cybersicurezza, con particolare riferimento alla necessità di assicurare una transizione digitale cyber resiliente della Pubblica Amministrazione (PA) e del tessuto produttivo, nonché di favorire Autonomia strategica nazionale ed europea nel settore del digitale;
- dalla Strategia Cloud Italia, la quale prevede che i servizi della pubblica amministrazione, in base alla criticità (ordinari, critici, strategici), siano erogati per mezzo di infrastrutture e servizi cloud con crescenti requisiti di sicurezza.
- dal Perimetro di sicurezza nazionale cibernetica (D.L. 105/2019), il quale prevede che i soggetti che svolgono funzioni essenziali dello Stato o erogano servizi essenziali debbano adottare appropriate misure di sicurezza sulle reti, sui sistemi informativi e sui servizi informatici (cd. bene ICT) necessari per lo svolgimento delle funzioni o dei servizi essenziali, notificare gli incidenti con impatto sul proprio bene ICT allo CSIRT Italia, nonché sottoporre l'affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati nel proprio bene ICT al processo di valutazione del CVCN.

La proposta è strutturata in modo analogo all'Artificial Intelligence Act (AIA)[1], definendo meccanismi in linea con quanto previsto dal New Legislative Framework[2]. In particolare, il Regolamento:

- caratterizza i "prodotti con elementi digitali" in quattro fasce di criticità (ordinari, critici di classe I, critici di classe II e altamente critici);
- definisce dei meccanismi di valutazione di conformità commisurati al livello di criticità del prodotto, dalle autocertificazioni alle certificazioni europee di cybersicurezza ai sensi del cd. Cybersecurity Act (CSA)[3];
- impone ai produttori di adottare migliore pratiche in materia di cybersicurezza nello sviluppo e nella manutenzione, specie con riferimento alla gestione delle vulnerabilità;
- prospetta le modalità di integrazione con le previsioni della Direttiva NIS2, nonché con numerose altre normative europee orizzontali impattate
- richiede agli Stati membri (SM) di individuare una autorità che svolga le procedure di accreditamento degli organismi di valutazione della conformità (conformity assesment bodies – CAB), nonché una o più autorità di vigilanza del mercato responsabili dell'attuazione nazionale del Regolamento.

La proposta di Regolamento colma una lacuna nell'impianto normativo europeo volto a rafforzare la cybersicurezza e la resilienza cyber dell'Unione, senza inficiare iniziative nazionali. Al contempo, il potenzialmente ampio ambito di applicazione e la necessaria integrazione nei meccanismi di vigilanza del mercato, nella normativa cyber vigente, nonché nelle ulteriori normative settoriali europee e nazionali, rendono il testo proposto ambizioso e delicato.

[1] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (COM(2021) 206 final del 21 aprile 2021).

[2] Il New Legislative Framework (NLF) rappresenta un pacchetto di misure volte a migliorare il funzionamento del mercato interno UE, rafforzando la vigilanza del mercato e la conformità dei prodotti (Regolamento (CE) 765/2008, Decisione 768/2008 del Parlamento europeo e del Consiglio, Regolamento (UE) 2019/1020).

[3] Citato Regolamento (UE) 2019/881 che definisce, tra l'altro, i sistemi europei di certificazione della cybersicurezza per i prodotti, servizi e processi ICT.

A. Rispetto dei principi dell'ordinamento europeo

1. Rispetto del principio di attribuzione, con particolare riguardo alla correttezza della base giuridica

La proposta rispetta il principio di attribuzione poiché l'Unione europea agirebbe nei limiti delle competenze che le sono attribuite dagli artt. da 2 a 6 del TFUE. La base giuridica è correttamente individuata nell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), che prevede l'adozione di misure atte a garantire l'instaurazione ed il funzionamento del mercato interno. L'obiettivo della proposta è armonizzare i requisiti di cybersicurezza per i prodotti con elementi digitali in tutti gli Stati membri e rimuovere gli ostacoli alla libera circolazione delle merci.

2. Rispetto del principio di sussidiarietà

La proposta rispetta il principio di sussidiarietà in quanto conforme all'articolo 5.3 del trattato sull'Unione europea (TUE) che esclude l'intervento dell'Unione quando una questione può essere regolata in modo efficace dagli Stati membri stessi a livello centrale, regionale o locale. Ciò anche in ragione degli aspetti transfrontalieri della cybersicurezza in generale e il numero crescente di rischi e incidenti, che hanno effetti di ricaduta a livello transfrontaliero, nonché dell'esistente impianto normativo europeo relativo alla vigilanza del mercato

3. Rispetto del principio di proporzionalità

La proposta appare rispettare il principio di proporzionalità in quanto conforme all'articolo 5.4 del trattato sull'Unione europea (TUE) che stabilisce che il contenuto e la forma dell'azione dell'Unione devono limitarsi a quanto necessario per il conseguimento degli obiettivi dei trattati. La proposta estensione del concetto di sorveglianza del mercato, rafforzato dal Regolamento (EU) 2019/1020, al dominio della cybersicurezza per i prodotti con elementi digitali, appare quanto mai necessario per promuovere una transizione digitale sicura.

B. Valutazione complessiva del progetto e delle sue prospettive negoziali

1. Valutazione del progetto e urgenza

La valutazione delle finalità generali del progetto è complessivamente positiva in quanto il Regolamento in oggetto è complementare, tramite l'introduzione degli aspetti di cybersicurezza nella sorveglianza di mercato, alle iniziative poste in essere a livello europeo e nazionale in materia di sicurezza della catena di approvvigionamento ICT, di cybersicurezza del mercato digitale e delle infrastrutture critiche, nonché di preparazione, prevenzione, risposta e ripristino ad incidenti e crisi di cybersicurezza.
Il progetto è di particolare urgenza in quanto pone le prime basi concrete per una gestione sicura e consapevole del ciclo di vita dei prodotti con elementi digitali, già nella fase di sviluppo e per la gestione responsabile delle vulnerabilità.

2. Conformità del progetto all'interesse nazionale

Le disposizioni contenute nel progetto possono ritenersi conformi all'interesse nazionale, in quanto in linea con le iniziative poste in essere dal nostro Paese in materia di cybersicurezza, in Italia e all'estero, consentendo di promuovere un livello di cybersicurezza rafforzato ed uniforme per i prodotti con elementi digitali, favorendo la concorrenza equa tra fornitori, nonché innalzando la cybersicurezza dei prodotti impiegati dai cittadini, dalle aziende e dalla pubblica amministrazione italiani.

3. Prospettive negoziali ed eventuali modifiche ritenute necessarie od opportune

Il Regolamento introduce numerosi elementi di novità nel panorama regolamentare e negoziale cyber e significative interazioni con molte altre normative europee orizzontali e settoriali. Pertanto, anche attesa la necessità di numerosi coordinamenti interministeriali e approfondimenti per opportunamente valutare gli impatti delle disposizioni, nonché loro modifiche in fase negoziale e alla luce delle prime indicazioni ricevute dall'attuale Presidenza di turno dell'UE, è ipotizzabile la chiusura della fase negoziale in Consiglio (cd. general agreement) tra giugno e dicembre 2023, con una pubblicazione in Gazzetta Ufficiale europea, a valle del cd. Trilogo, nel

2024.
In seno al gruppo di lavoro competente del Consiglio (Horizontal Working Party on Cyber Issues – HWPCI) sono già stati espressi primi elementi di valutazione, in particolare circa:

- la definizione di un modello di governo a livello europeo dell'implementazione del Regolamento, assicurando il necessario coinvolgimento degli Stati membri;
- la delicatezza dell'impianto definitorio proposto per evitare ambiguità circa l'ambito di applicazione;
- l'opportunità di assicurare adeguati requisiti, nonché meccanismi di gestione e segnalazione, in materia di vulnerabilità.

Inoltre, è di particolare rilevanza una attenta analisi per identificare l'opportuno bilanciamento tra livello di criticità dei prodotti e la severità dei requisiti di conformità e di certificazione richiesti, anche per addivenire ad un uso efficiente, oculato e complementare delle certificazioni di cybersicurezza previste dal cd. Cybersecurity Act (Regolamento (UE) 2019/881).
Con riferimento al rispetto dei principi dell'ordinamento europeo, si evidenzia che in fase negoziale sarà necessaria particolare attenzione a tutelare gli aspetti di cybersicurezza attinenti al dominio riservato, nonché assicurare un ragionevole periodo di transizione di 24 mesi, che darebbe tempo ai mercati interessati di prepararsi.

Tenuto conto di quanto rappresentato, sono già state avviate le dovute azioni, con il coordinamento delle Amministrazioni potenzialmente interessate, per la definizione di una posizione nazionale unitaria e coerente nel corso del negoziato europeo.

Si evidenzia, inoltre, che in vista della fase negoziale, Danimarca, Germania e Paesi Bassi hanno condiviso un non-paper, in linea di massima condivisibile, il quale auspica che il Regolamento:

- imponga un livello minimo di cybersicurezza, non derogabile da normative settoriali, le quali dovrebbero, invece, specializzare o innalzare i requisiti;
- comprenda l'intero ciclo di vita di tutti i prodotti, processi e servizi ICT, in linea con quanto previsto dal Cybersecurity Act (CSA) [1];
- definisca più livelli di cybersicurezza, analogamente al CSA, tra i quali i produttori possano scegliere quello con il quale intendano distribuire il proprio prodotto.

[1] Citato Regolamento (UE) 2019/881 che definisce, tra l'altro, i sistemi europei di certificazione della cybersicurezza per i prodotti, servizi e processi ICT.

C. Valutazione d'impatto

1. Impatto finanziario

Si ritiene opportuno evidenziare che per poter procedere ad una compiuta analisi degli oneri finanziari gravanti sul bilancio nazionale, appare necessario attendere i futuri sviluppi negoziali relativi al progetto di norma di cui trattasi, ciò in quanto fortemente dipendenti dall'accordo che verrà individuato circa l'ambito di applicazione, nonché circa il bilanciamento tra livello di criticità dei prodotti e la severità dei requisiti di conformità e di certificazione richiesti.

2. Effetti sull'ordinamento nazionale

La norma potrebbe richiedere adeguamenti, senza tuttavia presentare elementi di criticità, per:

- l'individuazione di un'autorità di notifica, responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione e la notifica degli organismi di valutazione della conformità e il controllo degli organismi notificati, nonché di un'autorità di vigilanza del mercato, responsabile per la vigilanza del mercato nel territorio dello Stato membro;
- l'eventuale raccordo con l'architettura nazionale cyber definita dal D.L. 82/2021, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, nonché la regolamentazione in materia di cybersicurezza (D.Lgs. 65/2018 e D.L. 105/2019 convertito con convertito con modificazioni dalla L. 18 novembre 2019, n. 133);

- l'eventuale raccordo con le disposizioni nazionali discendenti dal Regolamento (UE) 2019/1020, relative alla vigilanza del mercato.

3. Effetti sulle competenze regionali e delle autonomie locali

La norma non incide sulle competenze regionali e delle autonomie locali ai sensi di quanto previsto dalla Costituzione; pertanto, la relazione non dovrà essere inviata alle Regioni, per il tramite delle loro Conferenze (art. 24, comma 2, della legge n. 234/2012).

4. Effetti sull'organizzazione della pubblica amministrazione

La norma, non presentando elementi di criticità circa gli effetti sull'organizzazione della pubblica amministrazione, prevede l'individuazione di un'autorità di notifica, responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione e la notifica degli organismi di valutazione della conformità e il controllo degli organismi notificati, nonché di un'autorità di vigilanza del mercato, responsabile per la vigilanza del mercato nel territorio dello Stato membro. Al riguardo, sarà quindi necessario attribuire tali competenze ad uno o più enti pubblici nazionali, con l'eventuale necessità di prevedere opportune dotazioni finanziarie e organiche.

5. Effetti sulle attività dei cittadini e delle imprese

La norma avrà un impatto positivo sui cittadini e sulle imprese, le quali godranno di prodotti con elementi digitali con un livello di cybersicurezza più elevato, in termini di sviluppo e gestione del ciclo di vita, nonché di un mercato più equo e concorrenziale, a complemento del percorso di rafforzamento della resilienza cyber del mercato digitale europeo, quale pilastro indispensabile ad una transizione digitale responsabile.

Al contempo, in funzione del bilanciamento individuato tra criticità dei prodotti con elementi digitali e i dei requisiti di conformità e/o di certificazione richiesti, potrebbe verificarsi un incremento dei costi di produzione.

Altro

Si precisa che la proposta nella sua versione originale è suscettibile di essere modificata nel corso del negoziato nell'ambito delle competenti sedi istituzionali europee e che la posizione della nostra delegazione potrà evolvere, in base anche alle consultazioni con le amministrazioni e le parti interessate.

LOGO
Amministrazione
con competenza
prevalente

Tabella di corrispondenza
ai sensi dell'art. 6, comma 5, della legge n. 234/2012

(D.P.C.M. 17marzo 2015)

Oggetto dell'atto:
Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020

- **Codice della proposta:** COM(2022) 454 final del 16/09/2022
- **Codice interistituzionale:** 2022/0272(COD)
- **Amministrazione con competenza prevalente:** Presidenza del Consiglio dei ministri e Agenzia per la cybersicurezza nazionale

Disposizione del progetto di atto legislativo dell'Unione europea (articolo e paragrafo)	**Norma nazionale vigente** (norma primaria e secondaria)	**Commento** (natura primaria o secondaria della norma, competenza ai sensi dell'art. 117 della Costituzione, eventuali oneri finanziari, impatto sull'ordinamento nazionale, oneri amministrativi aggiuntivi, amministrazioni coinvolte, eventuale necessità di intervento normativo di natura primaria o secondaria)