Consiglio dell'Unione europea

Bruxelles, 16 settembre 2022
(OR. en)

12429/22

Fascicolo interistituzionale: 2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

PROPOSTA

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	15 settembre 2022
Destinatario:	Segretariato generale del Consiglio
n. doc. Comm.:	COM(2022) 454 final
Oggetto:	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

Si trasmette in allegato, per le delegazioni, il documento COM(2022) 454 final.

All.: COM(2022) 454 final

COMMISSIONE
EUROPEA

Bruxelles, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

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

(Testo rilevante ai fini del SEE)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

I prodotti hardware e software sono sempre più soggetti ad attacchi informatici andati a segno, e si stima che entro il 2021 il costo globale annuo della criminalità informatica ammonterà a 5 500 miliardi di EUR. Tali prodotti risentono di due problemi principali, che comportano ulteriori costi per gli utilizzatori e per la società: 1) un basso livello di cibersicurezza, testimoniato da vulnerabilità diffuse e dalla fornitura insufficiente e incoerente di aggiornamenti di sicurezza per porvi rimedio e 2) un'insufficiente comprensione delle informazioni e un accesso limitato alle stesse da parte degli utilizzatori, che impediscono loro di scegliere prodotti con proprietà di cibersicurezza adeguate o di utilizzarli in modo sicuro. In un ambiente connesso un incidente di cibersicurezza in un prodotto può pregiudicare un'intera organizzazione o un'intera catena di approvvigionamento, spesso propagandosi attraverso le frontiere del mercato interno nel giro di pochi minuti. Ciò può perturbare gravemente le attività economiche e sociali o persino diventare una minaccia letale.

La cibersicurezza dei prodotti con elementi digitali ha una forte dimensione transfrontaliera, poiché i prodotti fabbricati in un paese sono spesso utilizzati in tutto il mercato interno. Inoltre gli incidenti che inizialmente interessano un singolo soggetto o un singolo Stato membro spesso si diffondono in pochi minuti nell'intero mercato interno.

Sebbene la normativa vigente in materia di mercato interno si applichi ad alcuni prodotti con elementi digitali, la maggior parte dei prodotti hardware e software non è attualmente disciplinata da alcuna normativa dell'UE riguardante la loro cibersicurezza. In particolare l'attuale quadro giuridico dell'UE non affronta la questione della cibersicurezza del software non incorporato, anche se gli attacchi alla cibersicurezza prendono sempre più di mira le vulnerabilità di tali prodotti, causando costi sociali ed economici significativi. Esistono numerosi esempi di attacchi informatici di grande portata dovuti a una sicurezza non ottimale dei prodotti, come il worm ransomware WannaCry, che ha sfruttato una vulnerabilità di Windows, colpendo, nel 2017, 200 000 computer in 150 paesi e provocando danni per miliardi di dollari; l'attacco alla catena di approvvigionamento di Kaseya VSA, che ha utilizzato il software di amministrazione di rete di Kaseya per attaccare oltre 1 000 imprese, costringendo una catena di supermercati a chiudere tutti i suoi 500 negozi in Svezia; oppure i numerosi incidenti in cui sono violate le applicazioni bancarie per rubare denaro a consumatori ignari.

Sono stati individuati due obiettivi principali per garantire il corretto funzionamento del mercato interno: 1) creare le condizioni per lo sviluppo di prodotti con elementi digitali sicuri, garantendo che i prodotti hardware e software siano immessi sul mercato con un minor numero di vulnerabilità, e far sì che i fabbricanti prendano la sicurezza in seria considerazione durante l'intero ciclo di vita di un prodotto e 2) creare le condizioni che consentano agli utilizzatori di tenere conto della cibersicurezza nella scelta e nell'utilizzo dei prodotti con elementi digitali. Sono stati definiti quattro obiettivi specifici: i) 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; ii) garantire un quadro coerente in materia di cibersicurezza, facilitando la conformità per i produttori di hardware e software; iii) migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali e iv) consentire alle imprese e ai consumatori di utilizzarli in modo sicuro.

La forte natura transfrontaliera della cibersicurezza e i crescenti incidenti, con effetti di ricaduta a livello transfrontaliero e trasversalmente ai settori e ai prodotti, fanno sì che gli obiettivi non possano essere raggiunti efficacemente dai soli Stati membri. Data la natura globale dei mercati dei prodotti con elementi digitali, sul rispettivo territorio gli Stati membri si trovano ad affrontare gli stessi rischi per lo stesso prodotto con elementi digitali. Il formarsi di un quadro frammentato di norme nazionali potenzialmente divergenti rischia di ostacolare la creazione di un mercato unico aperto e competitivo per i prodotti con elementi digitali. È quindi necessaria un'azione comune a livello dell'UE per aumentare il grado di fiducia degli utilizzatori e l'attrattiva dei prodotti con elementi digitali dell'UE. Tale azione avrebbe anche benefici per il mercato interno, garantendo la certezza del diritto e creando condizioni di parità per i venditori di prodotti con elementi digitali, come evidenziato anche nella relazione finale della Conferenza sul futuro dell'Europa, in cui i cittadini chiedono un ruolo più incisivo dell'UE nella lotta contro le minacce alla cibersicurezza.

- **Interazione con le disposizioni vigenti nel settore normativo interessato**

Il quadro dell'UE comprende diversi atti legislativi orizzontali che trattano alcuni aspetti legati alla cibersicurezza da vari punti di vista (prodotti, servizi, gestione delle crisi e reati). Nel 2013 è entrata in vigore la direttiva relativa agli attacchi contro i sistemi di informazione[1], che armonizza la criminalizzazione e le sanzioni per una serie di reati diretti contro i sistemi di informazione. Nell'agosto 2016 è entrata in vigore la direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS)[2], che è il primo strumento legislativo a livello dell'UE sulla cibersicurezza. La sua revisione, concretizzatasi nella direttiva [direttiva XXX/XXXX (NIS2)], innalza il livello di ambizione comune dell'UE. Nel 2019 è entrato in vigore il regolamento sulla cibersicurezza dell'UE[3], che mira a migliorare la sicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC, introducendo un quadro volontario europeo di certificazione della cibersicurezza[4].

La cibersicurezza dell'intera catena di approvvigionamento è garantita solo se tutti i suoi componenti sono cibersicuri. La normativa dell'UE di cui sopra presenta tuttavia lacune sostanziali sotto questo profilo, in quanto non contempla requisiti obbligatori per la sicurezza dei prodotti con elementi digitali.

Mentre la proposta di legge sulla ciberresilienza riguarda i prodotti con elementi digitali immessi sul mercato, la direttiva [direttiva XXX/XXX (NIS2)] mira a garantire un livello elevato di cibersicurezza dei servizi forniti dai soggetti essenziali e importanti. La direttiva [direttiva XXX/XXXX (NIS2)] impone agli Stati membri di garantire che i soggetti essenziali e importanti che rientrano nell'ambito di applicazione, come i prestatori di assistenza sanitaria o i fornitori di servizi cloud e gli enti della pubblica amministrazione, adottino misure di

---

1 Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

2 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

3 Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

4 Il regolamento sulla cibersicurezza consente lo sviluppo di appositi sistemi di certificazione. Ciascun sistema include i riferimenti alle pertinenti norme o specifiche tecniche o ad altri requisiti di cibersicurezza definiti nel sistema. La decisione riguardo allo sviluppo di una certificazione della cibersicurezza è basata sul rischio.

cibersicurezza adeguate e proporzionate dal punto di vista tecnico, operativo e organizzativo. Ciò include, tra l'altro, l'obbligo di garantire la sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità. La direttiva [direttiva XXX/XXXX (NIS2)] impone alla Commissione di adottare atti di esecuzione che stabiliscano i requisiti tecnici e metodologici di tali misure entro 21 mesi dalla data di entrata in vigore di tale direttiva per alcuni tipi di soggetti, come i fornitori di servizi di cloud computing. Per tutti gli altri soggetti, la Commissione può adottare un atto di esecuzione che stabilisca i requisiti tecnici e metodologici, nonché i requisiti settoriali. Tale quadro garantirà che le misure e le specifiche tecniche simili ai requisiti essenziali di cibersicurezza della legge sulla ciberresilienza siano attuate anche per la progettazione, lo sviluppo e la gestione delle vulnerabilità del software fornito come servizio (servizio a livello di software). Ad esempio ciò potrebbe essere un mezzo per garantire un livello elevato di cibersicurezza in casi come quello dei sistemi di cartelle cliniche elettroniche, anche se forniti come servizio a livello di software (Software-as-a-Service – SaaS) o sviluppati all'interno delle istituzioni sanitarie (internamente), in conformità con la proposta di [regolamento sullo spazio europeo dei dati sanitari].

- **Interazione con le altre normative dell'Unione**

Come si legge nella comunicazione "Plasmare il futuro digitale dell'Europa"[5], è fondamentale che l'UE colga tutti i vantaggi dell'era digitale e rafforzi la sua industria e la sua capacità di innovazione entro limiti sicuri ed etici. La strategia europea per i dati stabilisce quattro pilastri, ovvero protezione dei dati, diritti fondamentali, sicurezza e cibersicurezza, come prerequisiti essenziali per una società che, grazie all'uso dei dati, disponga di maggiori strumenti.

Il quadro giuridico dell'UE[6] attualmente applicabile ai prodotti che possono avere anche elementi digitali comprende diversi atti legislativi, tra cui atti su prodotti specifici che disciplinano aspetti legati alla sicurezza e atti di portata generale sulla responsabilità per danno da prodotti difettosi. La proposta è coerente con l'attuale quadro normativo dell'UE relativo ai prodotti e con le recenti proposte legislative, come la proposta di regolamento presentata dalla Commissione [regolamento sull'intelligenza artificiale][7].

Il regolamento proposto si applicherebbe a tutte le apparecchiature radio che rientrano nell'ambito di applicazione del regolamento delegato (UE) 2022/30 della Commissione. Inoltre i requisiti stabiliti dal presente regolamento comprendono tutti gli elementi dei requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere d), e) e f), della direttiva 2014/53/UE, compresi gli elementi principali indicati nella [decisione di esecuzione XXX/2022 della Commissione relativa ad una richiesta di normazione rivolta alle organizzazioni europee di normazione] emessa sulla base di tale regolamento delegato. Al fine di evitare una sovrapposizione normativa, si prevede che la Commissione abroghi o modifichi il regolamento delegato con riguardo alle apparecchiature radio contemplate dalla proposta di regolamento, in modo tale che ad esse si applichi quest'ultimo regolamento, una volta applicabile.

---

5 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – "Plasmare il futuro digitale dell'Europa" (COM(2020) 67 final del 19 febbraio 2020).

6 Principalmente la legislazione del nuovo quadro normativo.

7 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).

Inoltre, al fine di evitare una duplicazione delle attività, si prevede che la Commissione e le organizzazioni europee di normazione tengano conto dei lavori di normazione svolti nel contesto della decisione di esecuzione C(2022)5637 della Commissione relativa ad una richiesta di normazione per il regolamento delegato (UE) 2022/30 che integra la direttiva sulle apparecchiature radio nella preparazione e nello sviluppo di norme armonizzate per facilitare l'attuazione del regolamento.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

• Base giuridica

La base giuridica della presente proposta è costituita dall'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 cibersicurezza per i prodotti con elementi digitali in tutti gli Stati membri e rimuovere gli ostacoli alla libera circolazione delle merci.

L'articolo 114 TFUE può essere utilizzato come base giuridica per prevenire l'insorgere di tali ostacoli risultanti da legislazioni e approcci nazionali divergenti per quanto riguarda la risoluzione delle incertezze e delle lacune giuridiche dei quadri giuridici esistenti[8]. Inoltre la Corte di giustizia ha riconosciuto che l'applicazione di requisiti tecnici eterogenei potrebbe essere un motivo valido per ricorrere all'articolo 114 TFUE[9].

Il quadro normativo dell'UE attualmente applicabile ai prodotti con elementi digitali si basa sull'articolo 114 TFUE e comprende diversi atti legislativi, tra cui atti su prodotti specifici e aspetti legati alla sicurezza o atti di portata generale sulla responsabilità per danno da prodotti difettosi. Tuttavia esso contempla solo alcuni aspetti legati alla cibersicurezza dei prodotti digitali tangibili e, se del caso, del software incorporato in tali prodotti. A livello nazionale gli Stati membri stanno iniziando ad adottare misure nazionali che richiedono ai venditori di prodotti digitali di migliorarne la cibersicurezza[10]. Al contempo la cibersicurezza dei prodotti digitali ha una dimensione transfrontaliera particolarmente forte, poiché i prodotti fabbricati in un paese sono spesso utilizzati da organizzazioni e consumatori in tutto il mercato interno. Gli incidenti che inizialmente riguardano un singolo soggetto o un singolo Stato membro spesso si diffondono in pochi minuti tra organizzazioni, settori e diversi Stati membri.

I vari atti adottati e le diverse iniziative intraprese finora a livello nazionale e dell'UE affrontano solo parzialmente i problemi individuati e rischiano di creare un mosaico legislativo all'interno del mercato interno, aumentando l'incertezza del diritto sia per i venditori sia per gli utilizzatori di tali prodotti e imponendo alle imprese un onere aggiuntivo inutile per conformarsi a una serie di requisiti per tipi di prodotti simili.

Il regolamento proposto armonizzerebbe e snellirebbe il panorama normativo dell'UE introducendo requisiti di cibersicurezza per i prodotti con elementi digitali ed eviterebbe la sovrapposizione di requisiti derivanti da diversi atti legislativi. Ciò creerebbe una maggiore certezza del diritto per gli operatori e gli utilizzatori in tutta l'Unione, nonché una migliore

---

8 Sentenza della Corte di giustizia (Grande Sezione) del 3 dicembre 2019, *Repubblica ceca/Parlamento europeo e Consiglio dell'Unione europea*, C-482/17, punto 35.

9 Sentenza della Corte di giustizia (Grande Sezione) del 2 maggio 2006, *Regno Unito di Gran Bretagna e Irlanda del Nord/Parlamento europeo e Consiglio dell'Unione europea*, C-217/04, punti 62-63.

10 Ad esempio nel 2019 la Finlandia ha creato un sistema di etichettatura per i dispositivi IoT, come smart TV, smartphone e giocattoli, basato sulle norme ETSI. La Germania ha recentemente introdotto un'etichetta di sicurezza per i consumatori per router a banda larga, smart TV, fotocamere, altoparlanti, giocattoli e robot per la pulizia e il giardinaggio.

armonizzazione del mercato unico europeo, garantendo condizioni più agevoli agli operatori che intendono entrare nel mercato dell'UE.

- **Sussidiarietà (per la competenza non esclusiva)**

La forte natura transfrontaliera della cibersicurezza in generale e il numero crescente di rischi e incidenti, che hanno effetti di ricaduta a livello transfrontaliero e trasversalmente ai settori e ai prodotti, fanno sì che gli obiettivi del presente intervento non possano essere raggiunti efficacemente dai soli Stati membri. Gli approcci nazionali adottati per affrontare i problemi, e in particolare gli approcci che introducono requisiti obbligatori, creeranno ulteriore incertezza del diritto e ostacoli giuridici. Alle imprese potrebbe essere impedito di espandersi senza soluzione di continuità in altri Stati membri, privando gli utilizzatori della possibilità di beneficiare dei loro prodotti.

È quindi necessaria un'azione comune a livello dell'UE per instaurare un livello elevato di fiducia tra gli utilizzatori, rafforzando inoltre l'attrattiva dei prodotti con elementi digitali dell'UE. Tale azione avrebbe anche benefici per il mercato unico digitale e per il mercato interno in generale, garantendo la certezza del diritto e creando condizioni di parità per i fabbricanti di prodotti con elementi digitali.

Infine le conclusioni del Consiglio del 23 maggio 2022 sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica invitano la Commissione a proporre, entro la fine del 2022, requisiti comuni in materia di cibersicurezza per i dispositivi connessi.

- **Proporzionalità**

Per quanto riguarda la proporzionalità del regolamento proposto, le misure delle opzioni strategiche considerate non andrebbero oltre quanto necessario per conseguire gli obiettivi generali e specifici e non imporrebbero costi sproporzionati. Più specificamente l'intervento preso in considerazione garantirebbe che i prodotti con elementi digitali siano protetti durante l'intero ciclo di vita e in modo proporzionale ai rischi affrontati attraverso requisiti orientati agli obiettivi e tecnologicamente neutri che rimangano ragionevoli e corrispondano generalmente agli interessi dei soggetti coinvolti.

I requisiti essenziali di cibersicurezza contenuti nella proposta si basano su norme ampiamente utilizzate e il processo di normazione che ne deriverebbe terrebbe conto delle specificità tecniche dei prodotti, con la conseguenza che, ove necessario per un determinato livello di rischio, i controlli di sicurezza sarebbero adattati. Inoltre le norme orizzontali previste contemplerebbero la valutazione da parte di terzi solo dei prodotti critici, il che riguarderebbe solo una piccola parte del mercato dei prodotti con elementi digitali. L'impatto sulle PMI dipenderebbe dalla loro presenza sul mercato di tali specifiche categorie di prodotti.

Per quanto riguarda la proporzionalità dei costi per la valutazione della conformità, gli organismi notificati che effettuano le valutazioni da parte di terzi terrebbero conto delle dimensioni dell'impresa nel fissare le loro tariffe. Per preparare l'attuazione sarebbe inoltre previsto un ragionevole periodo di transizione di 24 mesi, che darebbe tempo ai mercati interessati di prepararsi, fornendo al contempo una direzione chiara per gli investimenti in R&S. Gli eventuali costi di conformità per le imprese sarebbero compensati dai vantaggi derivanti da un maggiore livello di sicurezza dei prodotti con elementi digitali e, in ultima analisi, da un aumento della fiducia degli utilizzatori nei confronti di tali prodotti.

- **Scelta dell'atto giuridico**

Un intervento normativo richiederebbe l'adozione di un regolamento e non di una direttiva. La ragione è che, per questo particolare tipo di normativa sui prodotti, un regolamento sarebbe più efficace nell'affrontare i problemi individuati e nel raggiungere gli obiettivi formulati,

poiché si tratta di un intervento che condiziona l'immissione sul mercato interno di una categoria di prodotti molto ampia. Il processo di recepimento nel caso di una direttiva per questo tipo di intervento potrebbe lasciare troppo spazio alla discrezionalità a livello nazionale, portando potenzialmente alla mancanza di uniformità di taluni requisiti essenziali di cibersicurezza, all'incertezza del diritto, a un'ulteriore frammentazione o addirittura a situazioni discriminatorie a livello transfrontaliero, ancor più se si considera che i prodotti disciplinati potrebbero avere molteplici scopi o usi e che i fabbricanti possono produrre varie categorie di tali prodotti.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

• Consultazioni dei portatori di interessi

La Commissione ha consultato una vasta gamma di portatori di interessi. Gli Stati membri e i portatori di interessi sono stati invitati a partecipare alla consultazione pubblica aperta e alle indagini e ai seminari organizzati nel contesto di uno studio condotto da un consorzio a sostegno dei lavori preparatori della Commissione per la valutazione d'impatto: Wavestone, il Centro per gli studi politici europei (CEPS) e ICF. Tra i portatori di interessi consultati figurano le autorità nazionali di vigilanza del mercato, gli organismi dell'Unione preposti alla cibersicurezza, i fabbricanti di hardware e software, gli importatori e i distributori di hardware e software, le associazioni di categoria, le organizzazioni di consumatori e gli utilizzatori di prodotti con elementi digitali, i cittadini, i ricercatori e il mondo accademico, gli organismi notificati e gli organismi di accreditamento e i professionisti del settore della cibersicurezza.

Le attività di consultazione hanno compreso:

- un primo studio condotto da un consorzio composto da ICF, Wavestone, Carsa e CEPS, pubblicato nel dicembre 2021[11]. Lo studio ha individuato diverse carenze del mercato e valutato possibili interventi normativi;
- una consultazione pubblica aperta rivolta a cittadini, portatori di interessi ed esperti nel campo della cibersicurezza. Sono state inviate 176 risposte. Ciò ha contribuito alla raccolta di esperienze e pareri diversi da tutti i gruppi di portatori di interessi;
- i seminari organizzati dallo studio a sostegno dei lavori preparatori della Commissione per una legge sulla ciberresilienza hanno riunito circa 100 rappresentanti di tutti i 27 Stati membri, in rappresentanza di diversi portatori di interessi;
- sono state condotte interviste con esperti per comprendere più a fondo le attuali sfide in materia di cibersicurezza legate ai prodotti con elementi digitali e per discutere le opzioni strategiche per un possibile intervento normativo;
- si sono tenute discussioni bilaterali con le autorità nazionali di cibersicurezza, il settore privato e le organizzazioni di consumatori;
- è stata effettuata un'attività di sensibilizzazione mirata rivolta ai principali portatori di interessi delle PMI.

[11] Studio sulla necessità di requisiti di cibersicurezza per i prodotti TIC – n. 2020-0715, relazione finale dello studio, disponibile all'indirizzo https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products (solo in EN).

- **Assunzione e uso di perizie**

Le attività di consultazione erano volte a ottenere contributi sui cinque criteri di valutazione principali secondo gli orientamenti dell'UE per legiferare meglio (efficacia, efficienza, pertinenza, coerenza, valore aggiunto dell'UE), nonché sul potenziale impatto delle opzioni possibili per il futuro. Il contraente non solo ha contattato i portatori di interessi che sarebbero direttamente interessati dalla proposta di regolamento, ma ha anche consultato un'ampia gamma di esperti nel campo della cibersicurezza.

- **Valutazione d'impatto**

La Commissione ha condotto una valutazione d'impatto in relazione alla presente proposta, esaminata dal comitato per il controllo normativo della Commissione. Il 6 luglio 2022 si è tenuta una riunione con tale comitato, alla quale è seguito un parere positivo. La valutazione d'impatto è stata adattata per tener conto delle raccomandazioni e delle osservazioni del comitato.

La Commissione ha esaminato le differenti opzioni strategiche per conseguire l'obiettivo generale della proposta:

- approccio non vincolante (*soft law*) e misure volontarie (opzione 1). In questa opzione non vi sarebbe alcun intervento normativo obbligatorio. La Commissione pubblicherebbe invece comunicazioni, orientamenti, raccomandazioni ed eventualmente codici di condotta per incoraggiare l'adozione di misure volontarie. Continuerebbero a essere definiti regimi nazionali, volontari od obbligatori, per compensare la mancanza di norme orizzontali dell'UE;
- intervento normativo ad hoc per la cibersicurezza dei prodotti tangibili con elementi digitali e dei relativi software incorporati (opzione 2). Questa opzione comporterebbe un intervento normativo ad hoc specifico per prodotto, che si limiterebbe ad aggiungere e/o a modificare i requisiti di cibersicurezza nella normativa già esistente o a introdurre una nuova normativa laddove emergano nuovi rischi, eventualmente anche riguardo al software non incorporato.

Le opzioni 3 e 4 comportano un intervento normativo orizzontale di portata variabile, che segue in larga misura il nuovo quadro normativo. Tale quadro stabilisce requisiti essenziali come condizione per l'immissione sul mercato interno di determinati prodotti. Il nuovo quadro normativo prevede inoltre la valutazione della conformità, ossia il processo condotto dal fabbricante per dimostrare se i requisiti specifici connessi a un prodotto sono stati soddisfatti.

- Approccio misto comprendente norme obbligatorie orizzontali per la cibersicurezza dei prodotti tangibili con elementi digitali e dei relativi software incorporati e un approccio scaglionato per il software non incorporato (opzione 3): questa opzione comporterebbe un regolamento che introduca requisiti orizzontali di cibersicurezza per tutti i prodotti tangibili con elementi digitali e per il software in essi incorporato, come condizione per l'immissione sul mercato, e includerebbe due sotto-opzioni con e senza valutazione obbligatoria da parte di terzi (3i e 3ii). Il software non incorporato non sarebbe regolamentato.
- Un intervento normativo orizzontale che introduce requisiti di cibersicurezza per un'ampia gamma di prodotti tangibili e non tangibili con elementi digitali, compreso il software non incorporato (opzione 4): questa opzione assomiglia

all'opzione 3, ad eccezione dell'ambito di applicazione. L'opzione 4 comprenderebbe nell'ambito di applicazione di un eventuale regolamento il software non incorporato (con due sotto-opzioni che includono rispettivamente solo i software critici (4a) o tutti i software (4b)). Per ciascuna sotto-opzione sarebbero prese in considerazione le stesse sotto-opzioni relative alla valutazione della conformità dell'opzione 3.

Sulla base della valutazione dell'efficacia rispetto agli obiettivi specifici e dell'efficienza dei costi rispetto ai benefici, l'opzione prescelta è stata l'opzione 4 (con sotto-opzioni che riguardano tutti i software e che prevedono la valutazione obbligatoria da parte di terzi dei prodotti critici). Questa opzione garantirebbe la definizione di specifici requisiti orizzontali di cibersicurezza per tutti i prodotti con elementi digitali che sono immessi o messi a disposizione sul mercato interno e sarebbe l'unica opzione che considera l'intera catena di approvvigionamento digitale. Anche il software non incorporato, spesso esposto a vulnerabilità, rientrerebbe in tale intervento normativo, garantendo così un approccio coerente nei confronti di tutti i prodotti con elementi digitali, con una chiara ripartizione delle responsabilità dei vari operatori economici.

Questa opzione strategica conferisce anche un valore aggiunto, in quanto comprende gli aspetti relativi al dovere di diligenza e all'intero ciclo di vita dopo l'immissione sul mercato dei prodotti con elementi digitali, per garantire, tra l'altro, informazioni adeguate sull'assistenza di sicurezza e la fornitura di aggiornamenti di sicurezza. Questa opzione strategica consentirebbe inoltre di integrare nel modo più efficace la recente revisione del quadro NIS, garantendo i prerequisiti per una maggiore sicurezza della catena di approvvigionamento.

L'opzione prescelta apporterebbe benefici significativi ai vari portatori di interessi. Per le imprese, eviterebbe norme di sicurezza divergenti per i prodotti con elementi digitali, ridurrebbe i costi di conformità alla relativa normativa in materia di cibersicurezza e diminuirebbe il numero di incidenti informatici, i costi di gestione degli incidenti e i danni alla reputazione. Per l'intera UE si stima che l'iniziativa potrebbe comportare una riduzione dei costi degli incidenti che interessano le imprese di circa 180-290 miliardi di EUR all'anno. Determinerebbe inoltre un aumento del fatturato grazie alla diffusione della domanda di prodotti con elementi digitali e migliorerebbe la reputazione delle imprese a livello mondiale, portando a un aumento della domanda anche da fuori l'UE. Per gli utilizzatori l'opzione prescelta aumenterebbe la trasparenza delle proprietà di sicurezza e faciliterebbe l'uso dei prodotti con elementi digitali. I consumatori e i cittadini beneficerebbero inoltre di una migliore tutela dei loro diritti fondamentali, come la protezione della vita privata e dei dati.

Alla richiesta di valutare l'efficacia degli interventi strategici, i partecipanti alla consultazione pubblica hanno concordato che l'opzione 4 sarebbe la misura più efficace (4,08 su una scala da 1 a 5). Tra questi figurano le organizzazioni di consumatori (5,00), i partecipanti che si identificano come utilizzatori (4,22), gli organismi notificati (4,17), le autorità di vigilanza del mercato (5,00) e i produttori di prodotti con elementi digitali (3,85), compresi quelli di piccole e medie dimensioni (4,05).

- **Efficienza normativa e semplificazione**

La proposta stabilisce i requisiti da applicare ai fabbricanti di software e hardware. È necessario garantire la certezza del diritto ed evitare un'ulteriore frammentazione del mercato per quanto riguarda i requisiti di cibersicurezza relativi ai prodotti sul mercato interno, come dimostrato dall'ampio sostegno dei vari portatori di interessi a favore di un intervento orizzontale. La proposta ridurrà al minimo gli oneri normativi imposti ai fabbricanti da diversi

atti in materia di sicurezza dei prodotti. L'allineamento rispetto al nuovo quadro normativo significa un funzionamento migliore dell'intervento e della sua applicazione. La proposta razionalizza il processo di procedure di salvaguardia, coinvolgendo fabbricanti e Stati membri prima che la Commissione riceva notifiche. Gran parte dei fabbricanti che rientrano nell'ambito di applicazione della proposta ha già familiarità con il funzionamento del nuovo quadro normativo, il che contribuirà alla sua comprensione e attuazione. Per i consumatori e le imprese la proposta promuoverà la fiducia nei confronti dei prodotti con elementi digitali.

- **Diritti fondamentali**

Tutte le opzioni strategiche dovrebbero migliorare in una certa misura la tutela dei diritti e delle libertà fondamentali, come la protezione della vita privata e dei dati personali, la libertà d'impresa e la protezione della proprietà o la dignità e l'integrità della persona. In particolare l'opzione prescelta 4, caratterizzata da interventi normativi orizzontali e da un'ampia portata strategica, sarebbe la più efficace sotto questo profilo, in quanto è più probabile che contribuisca a ridurre il numero e la gravità degli incidenti, comprese le violazioni dei dati personali. Inoltre aumenterebbe la certezza del diritto e creerebbe condizioni di parità per gli operatori economici, rafforzerebbe la fiducia degli utilizzatori e l'attrattiva dei prodotti con elementi digitali dell'UE nel loro complesso, proteggendo così la proprietà e migliorando le condizioni degli operatori economici nella conduzione d'impresa.

I requisiti orizzontali di cibersicurezza contribuirebbero alla sicurezza dei dati personali proteggendo la riservatezza, l'integrità e la disponibilità delle informazioni nei prodotti con elementi digitali. L'osservanza di tali requisiti faciliterà il rispetto dell'obbligo di garantire la sicurezza del trattamento dei dati personali a norma del regolamento generale sulla protezione dei dati (GDPR)[12]. La proposta migliorerebbe la trasparenza e le informazioni fornite agli utilizzatori, anche a quelli che potrebbero disporre di minori competenze in materia di cibersicurezza. Gli utilizzatori sarebbero inoltre meglio informati sui rischi, sulle capacità e sui limiti dei prodotti con elementi digitali, e sarebbero dunque maggiormente in grado di adottare le necessarie misure preventive e di attenuazione per ridurre i rischi residui.

4. INCIDENZA SUL BILANCIO

Al fine di espletare i compiti che le sono conferiti dal presente regolamento, l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) dovrà riassegnare risorse pari a circa 4,5 ETP. La Commissione dovrebbe destinare 7 ETP all'adempimento delle sue responsabilità relative all'applicazione del presente regolamento.

Una panoramica dettagliata dei costi in questione è riportata nella "scheda finanziaria" collegata alla presente proposta.

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

La Commissione monitorerà l'attuazione, l'applicazione e il rispetto di queste nuove disposizioni al fine di valutarne l'efficacia. Il regolamento richiederà una valutazione e un riesame da parte della Commissione così come la presentazione di una relazione pubblica a

[12] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

tale riguardo al Parlamento europeo e al Consiglio entro 36 mesi dalla data di applicazione e successivamente ogni quattro anni.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

Disposizioni generali (capo I)

La presente proposta di regolamento stabilisce a) norme per l'immissione sul mercato di prodotti con elementi digitali per garantire la cibersicurezza di tali prodotti; b) requisiti essenziali per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali e obblighi per gli operatori economici in relazione a tali prodotti per quanto riguarda la cibersicurezza; c) requisiti essenziali per i processi di gestione delle vulnerabilità messi in atto dai fabbricanti per garantire la cibersicurezza dei prodotti con elementi digitali durante l'intero ciclo di vita e obblighi per gli operatori economici in relazione a tali processi; d) norme sulla vigilanza del mercato e sull'applicazione delle norme e dei requisiti di cui sopra.

Il regolamento proposto si applicherà a tutti i prodotti con elementi digitali il cui uso previsto e ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete.

Il regolamento proposto non si applicherà ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento (UE) 2017/745 [dispositivi medici per uso umano e accessori per tali dispositivi] e del regolamento (UE) 2017/746 [dispositivi medico-diagnostici *in vitro* per uso umano e accessori per tali dispositivi], in quanto entrambi i regolamenti contengono requisiti relativi ai dispositivi, anche in merito al software, e obblighi generali per i fabbricanti, che riguardano l'intero ciclo di vita dei prodotti, nonché procedure di valutazione della conformità. Il presente regolamento non si applica ai prodotti con elementi digitali che sono stati certificati in conformità del regolamento 2018/1139 [livello elevato ed uniforme di sicurezza dell'aviazione civile], né ai prodotti a cui si applica il regolamento (UE) 2019/2144 [relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli].

I prodotti con elementi digitali critici sono soggetti a specifiche procedure di valutazione della conformità e sono suddivisi in classi (classe I e classe II), come indicato nell'allegato III, le quali riflettono il loro livello di rischio di cibersicurezza (la classe II rappresenta un rischio maggiore). Un prodotto con elementi digitali è considerato critico, e quindi incluso nell'allegato III, tenendo conto dell'impatto delle potenziali vulnerabilità di cibersicurezza incluse nel prodotto con elementi digitali. Per la determinazione del rischio di cibersicurezza si tiene conto, tra l'altro, della funzionalità legata alla cibersicurezza del prodotto con elementi digitali e dell'uso previsto in ambienti sensibili come quelli industriali.

Alla Commissione è inoltre conferito il potere di adottare atti delegati per integrare il presente regolamento, specificando le categorie di prodotti con elementi digitali altamente critici per i quali i fabbricanti sono tenuti a ottenere un certificato europeo di cibersicurezza nell'ambito di un sistema europeo di certificazione della cibersicurezza per dimostrare la conformità ai requisiti essenziali di cui all'allegato I o a loro parti. Nel determinare tali categorie di prodotti con elementi digitali altamente critici, la Commissione tiene conto del livello di rischio di cibersicurezza relativo alla categoria di prodotti con elementi digitali, alla luce di uno o più dei criteri considerati per l'inserimento nell'elenco dei prodotti con elementi digitali critici di cui all'allegato III, nonché in considerazione della valutazione se tale categoria di prodotti sia utilizzata dai soggetti essenziali del tipo di cui all'allegato [allegato I] della direttiva [direttiva XXX/XXXX (NIS2)], sia una categoria di prodotti su cui detti soggetti fanno affidamento oppure possa avere un'importanza futura per le attività di tali soggetti, o sia pertinente per la

resilienza dell'intera catena di approvvigionamento dei prodotti con elementi digitali contro eventi perturbatori.

Obblighi degli operatori economici (capo II)

La proposta integra obblighi per i fabbricanti, gli importatori e i distributori sulla base delle disposizioni di riferimento previste dalla decisione 768/2008/CE. I requisiti e gli obblighi essenziali di cibersicurezza stabiliscono che tutti i prodotti con elementi digitali sono messi a disposizione sul mercato soltanto se, qualora siano debitamente forniti, correttamente installati, oggetto di un'adeguata manutenzione e utilizzati conformemente alla loro finalità prevista o in condizioni ragionevolmente prevedibili, soddisfano i requisiti essenziali di cibersicurezza prescritti dal presente regolamento.

I requisiti e gli obblighi essenziali imporrebbero ai fabbricanti di tenere conto della cibersicurezza nella progettazione, nello sviluppo e nella produzione di prodotti con elementi digitali, di esercitare la dovuta diligenza sugli aspetti di sicurezza durante la progettazione e lo sviluppo dei loro prodotti, di essere trasparenti sugli aspetti di cibersicurezza che devono essere resi noti ai clienti, di garantire assistenza di sicurezza (aggiornamenti) in modo proporzionato e di soddisfare i requisiti di gestione delle vulnerabilità.

La proposta stabilirebbe obblighi per gli operatori economici, a partire dai fabbricanti, fino ai distributori e agli importatori, in relazione all'immissione sul mercato di prodotti con elementi digitali, in funzione del loro ruolo e delle loro responsabilità nella catena di approvvigionamento.

Conformità del prodotto con elementi digitali (capo III)

Il prodotto con elementi digitali conforme alle norme armonizzate o a parti di esse, i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, si presume conforme ai requisiti essenziali di cui al presente regolamento. Qualora non esistano norme armonizzate o tali norme siano insufficienti o vi siano ritardi indebiti nella procedura di normazione o la richiesta della Commissione non sia stata accolta dalle organizzazioni europee di normazione, la Commissione può, mediante atti di esecuzione, adottare specifiche comuni.

Inoltre i prodotti con elementi digitali che sono stati certificati o per i quali sono stati rilasciati un certificato o una dichiarazione di conformità UE nell'ambito di un sistema europeo di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881, e per il quale la Commissione ha specificato, mediante atto di esecuzione, che può conferire una presunzione di conformità al presente regolamento, si presumono conformi ai requisiti essenziali del presente regolamento, o a parti di essi, nella misura in cui detti requisiti siano contemplati dal certificato di cibersicurezza o dalla dichiarazione di conformità UE, o da loro parti.

Inoltre, al fine di evitare un onere amministrativo indebito a carico dei fabbricanti, la Commissione dovrebbe specificare, ove applicabile, se un certificato di cibersicurezza rilasciato nell'ambito di un tale sistema europeo di certificazione della cibersicurezza sopprime l'obbligo per i fabbricanti di effettuare una valutazione della conformità da parte di terzi, come previsto dal presente regolamento per i requisiti corrispondenti.

Il fabbricante effettua una valutazione della conformità del prodotto con elementi digitali e dei processi di gestione delle vulnerabilità che ha messo in atto per dimostrare la conformità ai requisiti essenziali di cui all'allegato I, avvalendosi di una delle procedure di cui all'allegato VI. I fabbricanti di prodotti critici di classe I e II utilizzano i rispettivi moduli necessari ai fini della conformità. I fabbricanti di prodotti critici di classe II devono coinvolgere terzi nella valutazione della conformità.

Notifica degli organismi di valutazione della conformità (capo IV)

Un buon funzionamento degli organismi notificati è molto importante per ottenere livelli elevati di cibersicurezza, così come per la fiducia di tutte le parti interessate nel sistema del nuovo approccio. Di conseguenza, in linea con la decisione 768/2008/CE, la proposta stabilisce requisiti per le autorità nazionali responsabili degli organismi di valutazione della conformità (organismi notificati). Lascia la responsabilità ultima per quanto riguarda la designazione e il controllo degli organismi notificati agli Stati membri. Gli Stati membri designano 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.

Vigilanza del mercato e applicazione delle norme (capo V)

Conformemente al regolamento (UE) 2019/1020, le autorità nazionali di vigilanza del mercato effettuano la vigilanza del mercato nel territorio del rispettivo Stato membro. Gli Stati membri possono scegliere di designare qualsiasi autorità già esistente o una nuova autorità che agisca come autorità di vigilanza del mercato, comprese le autorità nazionali competenti di cui all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)] o le autorità nazionali di certificazione della cibersicurezza designate di cui all'articolo 58 del regolamento (UE) 2019/881. Gli operatori economici sono invitati a collaborare pienamente con le autorità di vigilanza del mercato e con le altre autorità competenti.

Delega di potere e procedura di comitato (capo VI)

Al fine di garantire che il quadro normativo possa essere adattato ove necessario, alla Commissione è delegato il potere di adottare atti conformemente all'articolo 290 TFUE per aggiornare l'elenco dei prodotti critici delle classi I e II e specificare le definizioni di tali prodotti, specificare se è necessaria una limitazione o un'esclusione per i prodotti con elementi digitali disciplinati da altre norme dell'Unione che stabiliscono requisiti che conseguono lo stesso livello di protezione del presente regolamento; imporre la certificazione di determinati prodotti con elementi digitali altamente critici sulla base dei criteri stabiliti nel presente regolamento, specificare il contenuto minimo della dichiarazione di conformità UE e integrare gli elementi da includere nella documentazione tecnica.

Alla Commissione è conferito inoltre il potere di adottare atti di esecuzione per: precisare il formato o gli elementi degli obblighi di segnalazione e della distinta base del software, specificare i sistemi europei di certificazione della cibersicurezza che possono essere utilizzati per dimostrare la conformità ai requisiti essenziali o a loro parti, come stabilito nel presente regolamento, adottare specifiche comuni, stabilire specifiche tecniche per l'apposizione della marcatura CE, adottare misure correttive o restrittive a livello di Unione in circostanze eccezionali che giustifichino un intervento immediato per preservare il buon funzionamento del mercato interno.

Riservatezza e sanzioni (capo VII)

Tutte le parti che applicano il presente regolamento rispettano la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività.

Per garantire l'effettiva applicazione degli obblighi previsti dal presente regolamento, ogni autorità di vigilanza del mercato dovrebbe avere il potere di imporre o richiedere l'imposizione di sanzioni amministrative pecuniarie. Allo stesso modo il presente regolamento stabilisce i livelli massimi delle sanzioni amministrative pecuniarie che dovrebbero essere previste negli ordinamenti nazionali in caso di mancato rispetto degli obblighi stabiliti dal presente regolamento.

Disposizioni transitorie e finali (capo VIII)

Affinché i fabbricanti, gli organismi notificati e gli Stati membri abbiano il tempo necessario per adeguarsi ai nuovi requisiti, il regolamento proposto sarà applicabile [24 mesi] dopo la sua entrata in vigore, ad eccezione dell'obbligo di segnalazione per i fabbricanti, che si applicherebbe a decorrere da [12 mesi] dopo la data di entrata in vigore.

2022/0272 (COD)

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

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[1],

visto il parere del Comitato delle regioni[2],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Occorre migliorare il funzionamento del mercato interno, definendo un quadro giuridico uniforme per i requisiti essenziali di cibersicurezza per l'immissione sul mercato dell'Unione di prodotti con elementi digitali. È opportuno affrontare i due problemi principali che comportano ulteriori costi per gli utilizzatori e la società: un basso livello di cibersicurezza dei prodotti con elementi digitali, testimoniato da vulnerabilità diffuse e dalla fornitura insufficiente e incoerente di aggiornamenti di sicurezza per porvi rimedio così come un'insufficiente comprensione delle informazioni e un accesso limitato alle stesse da parte degli utilizzatori, che impediscono loro di scegliere prodotti con proprietà di cibersicurezza adeguate o di utilizzarli in modo sicuro.

(2) Il presente regolamento mira a stabilire le condizioni limite per lo sviluppo di prodotti con elementi digitali sicuri, garantendo che i prodotti hardware e software siano immessi sul mercato con un minor numero di vulnerabilità e che i fabbricanti prendano la sicurezza in seria considerazione durante l'intero ciclo di vita di un prodotto. Si propone inoltre di creare le condizioni che consentano agli utilizzatori di tenere conto della cibersicurezza nella scelta e nell'utilizzo dei prodotti con elementi digitali.

(3) La normativa dell'Unione pertinente attualmente in vigore comprende diverse serie di norme orizzontali che affrontano taluni aspetti legati alla cibersicurezza da diversi punti di vista, comprese misure per migliorare la sicurezza della catena di approvvigionamento digitale. Tuttavia la normativa dell'Unione vigente in materia di

[1] GU C […] del […], pag. […].
[2] GU C […] del […], pag. […].

cibersicurezza, tra cui [la direttiva XXX/XXXX (NIS2)] e il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[3], non contempla direttamente requisiti obbligatori per la sicurezza dei prodotti con elementi digitali.

(4) Sebbene la normativa dell'Unione vigente si applichi a determinati prodotti con elementi digitali, non esiste un quadro normativo orizzontale dell'Unione che stabilisca requisiti di cibersicurezza completi per tutti i prodotti con elementi digitali. I vari atti adottati e le diverse iniziative intraprese finora a livello nazionale e dell'Unione affrontano solo parzialmente i problemi e i rischi individuati in materia di cibersicurezza, creando un mosaico legislativo all'interno del mercato interno, aumentando l'incertezza del diritto sia per i fabbricanti sia per gli utilizzatori di tali prodotti e imponendo alle imprese un onere aggiuntivo inutile per conformarsi a una serie di requisiti per tipi di prodotti simili. La cibersicurezza di tali prodotti ha una dimensione transfrontaliera particolarmente forte, poiché i prodotti fabbricati in un paese sono spesso utilizzati da organizzazioni e consumatori in tutto il mercato interno. Ciò rende necessaria una regolamentazione del settore a livello dell'Unione. Il panorama normativo dell'Unione dovrebbe essere armonizzato introducendo requisiti di cibersicurezza per i prodotti con elementi digitali. Inoltre si dovrebbe garantire la certezza del diritto per gli operatori e gli utilizzatori in tutta l'Unione, nonché una migliore armonizzazione del mercato unico, creando condizioni più agevoli per gli operatori che intendono entrare nel mercato dell'Unione.

(5) A livello dell'Unione diversi documenti programmatici e politici, come la strategia dell'UE in materia di cibersicurezza per il decennio digitale[4], le conclusioni del Consiglio del 2 dicembre 2020 e del 23 maggio 2022 o la risoluzione del Parlamento europeo del 10 giugno 2021[5], hanno chiesto l'introduzione di requisiti specifici dell'Unione in materia di cibersicurezza per i prodotti digitali o connessi e diversi paesi nel mondo hanno adottato di propria iniziativa misure volte ad affrontare la questione. Nella relazione finale della Conferenza sul futuro dell'Europa[6], i cittadini hanno chiesto "un ruolo più incisivo dell'UE nella lotta contro le minacce alla cibersicurezza".

(6) Per aumentare il livello generale di cibersicurezza di tutti i prodotti con elementi digitali immessi sul mercato interno è necessario introdurre requisiti essenziali di cibersicurezza orientati agli obiettivi e tecnologicamente neutri per tali prodotti, applicabili orizzontalmente.

(7) In determinate condizioni tutti i prodotti con elementi digitali integrati in un sistema di informazione elettronico più ampio o connessi a un tale sistema possono fungere da vettore di attacco per soggetti malintenzionati. Di conseguenza anche l'hardware e il software che sono considerati meno critici possono facilitare la compromissione iniziale di un dispositivo o di una rete, consentendo a soggetti malintenzionati di

---

3 Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=JOIN:2020:18:FIN.

5 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_IT.html.

6 Conferenza sul futuro dell'Europa – Relazione sul risultato finale, maggio 2022, proposta n. 28, punto 2. La Conferenza, tenutasi tra aprile 2021 e maggio 2022, ha costituito un esercizio unico guidato dai cittadini di democrazia deliberativa a livello paneuropeo, cui hanno partecipato migliaia di cittadini europei nonché attori politici, parti sociali, rappresentanti della società civile e i principali portatori di interessi.

ottenere un accesso privilegiato a un sistema o di muoversi lateralmente tra sistemi. I fabbricanti dovrebbero pertanto garantire che tutti i prodotti con elementi digitali collegabili siano progettati e sviluppati conformemente ai requisiti essenziali stabiliti nel presente regolamento. Sono compresi sia i prodotti che possono essere connessi in modo fisico tramite interfacce hardware sia i prodotti che sono connessi in modo logico, ad esempio tramite socket di rete, *pipe*, file, interfacce per programmi applicativi o qualsiasi altro tipo di interfaccia software. Poiché le minacce alla cibersicurezza possono propagarsi attraverso vari prodotti con elementi digitali prima di raggiungere un determinato obiettivo, ad esempio concatenando più exploit di vulnerabilità, i fabbricanti dovrebbero garantire la cibersicurezza anche dei prodotti che sono connessi solo indirettamente ad altri dispositivi o reti.

(8) Stabilendo requisiti di cibersicurezza per l'immissione sul mercato di prodotti con elementi digitali, si migliorerà la cibersicurezza di questi prodotti sia per i consumatori che per le imprese. Ciò include anche requisiti per l'immissione sul mercato di prodotti di consumo con elementi digitali destinati ai consumatori vulnerabili, come giocattoli e baby monitor.

(9) Il presente regolamento garantisce un livello elevato di cibersicurezza dei prodotti con elementi digitali. Esso non disciplina i servizi, come il servizio a livello di software (Software-as-a-Service – SaaS), ad eccezione delle soluzioni di elaborazione dati da remoto relative a un prodotto con elementi digitali, intese come una qualsiasi elaborazione dati a distanza per la quale il software è progettato e sviluppato dal fabbricante del prodotto in questione o sotto la sua responsabilità e la cui assenza impedirebbe a tale prodotto con elementi digitali di svolgere una delle sue funzioni. La [direttiva XXX/XXXX (NIS2)] stabilisce requisiti di cibersicurezza e di segnalazione degli incidenti per i soggetti essenziali e importanti, come le infrastrutture critiche, al fine di aumentare la resilienza dei servizi che forniscono. La [direttiva XXX/XXXX (NIS2)] si applica ai servizi di cloud computing e ai modelli di servizi cloud, come il SaaS. Tutti i soggetti che forniscono servizi di cloud computing nell'Unione e che raggiungono o superano la soglia per le medie imprese rientrano nell'ambito di applicazione di tale direttiva.

(10) Al fine di non ostacolare l'innovazione o la ricerca, il presente regolamento non dovrebbe disciplinare il software libero e open source sviluppato o fornito al di fuori di un'attività commerciale. Ciò vale in particolare per il software (compresi il codice sorgente e le versioni modificate) condiviso apertamente e liberamente accessibile, utilizzabile, modificabile e ridistribuibile. Nel contesto del software, un'attività commerciale può essere caratterizzata non solo dall'applicazione di un prezzo per un prodotto, ma anche dall'applicazione di un prezzo per i servizi di assistenza tecnica, dalla fornitura di una piattaforma software attraverso la quale il fabbricante monetizza altri servizi o dall'utilizzo di dati personali per motivi diversi dal solo miglioramento della sicurezza, della compatibilità o dell'interoperabilità del software.

(11) Lo sviluppo di un'internet sicura è indispensabile per il funzionamento delle infrastrutture critiche e per la società nel suo complesso. La [direttiva XXX/XXXX (NIS2)] mira a garantire un livello elevato di cibersicurezza dei servizi forniti dai soggetti essenziali e importanti, compresi i fornitori di infrastrutture digitali che sostengono le funzioni fondamentali dell'internet aperta e garantiscono i servizi internet e l'accesso a internet. È quindi importante che i prodotti con elementi digitali necessari ai fornitori di infrastrutture digitali per garantire il funzionamento di internet siano sviluppati in modo sicuro e siano conformi a norme di sicurezza internet consolidate. Il presente regolamento, che si applica a tutti i prodotti hardware e

software collegabili, mira anche a facilitare il rispetto dei requisiti relativi alla catena di approvvigionamento a norma della [direttiva XXX/XXXX (NIS2)] da parte dei fornitori di infrastrutture digitali, garantendo che i prodotti con elementi digitali che essi utilizzano per la fornitura dei loro servizi siano sviluppati in modo sicuro e che abbiano accesso ad aggiornamenti di sicurezza tempestivi per tali prodotti.

(12) Il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio[7] stabilisce norme relative ai dispositivi medici e il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio[8] stabilisce norme relative ai dispositivi medico-diagnostici *in vitro*. Entrambi i regolamenti si occupano di rischi di cibersicurezza e adottano approcci specifici che sono trattati anche nel presente regolamento. Più in particolare i regolamenti (UE) 2017/745 e (UE) 2017/746 stabiliscono i requisiti essenziali per i dispositivi medici che funzionano attraverso un sistema elettronico o che sono essi stessi software. Tali regolamenti disciplinano anche alcuni software non incorporati e l'approccio dell'intero ciclo di vita. Questi requisiti impongono ai fabbricanti di sviluppare e costruire i loro prodotti applicando principi di gestione del rischio e definendo requisiti relativi alle misure di sicurezza informatica, nonché corrispondenti procedure di valutazione della conformità. Inoltre da dicembre 2019 sono in vigore orientamenti specifici sulla cibersicurezza per i dispositivi medici, che forniscono ai fabbricanti di dispositivi medici, inclusi i dispositivi diagnostici *in vitro*, indicazioni su come soddisfare tutti i requisiti essenziali pertinenti dell'allegato I di tali regolamenti per quanto riguarda la cibersicurezza[9]. I prodotti con elementi digitali a cui si applica uno dei due regolamenti non dovrebbero pertanto essere soggetti al presente regolamento.

(13) Il regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio[10] stabilisce i requisiti per l'omologazione dei veicoli e dei loro sistemi e componenti, introducendo taluni requisiti di cibersicurezza riguardanti, tra l'altro, il funzionamento di un sistema certificato di gestione della cibersicurezza e gli aggiornamenti del software, disciplinando le politiche e i processi delle organizzazioni per i rischi informatici relativi all'intero ciclo di vita dei veicoli, dei dispositivi e dei servizi in conformità dei regolamenti delle Nazioni Unite applicabili in materia di specifiche tecniche e

---

7 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 (GU L 117 del 5.5.2017, pag. 1).

8 Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici *in vitro* e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

9 MDCG 2019-16, approvato dal gruppo di coordinamento per i dispositivi medici (MDCG) istituito dall'articolo 103 del regolamento (UE) 2017/745.

10 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 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 utenti vulnerabili della strada, che modifica il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio e abroga i regolamenti (CE) n. 78/2009, (CE) n. 79/2009 e (CE) n. 661/2009 del Parlamento europeo e del Consiglio e i regolamenti della Commissione (CE) n. 631/2009, (UE) n. 406/2010, (UE) n. 672/2010, (UE) n. 1003/2010, (UE) n. 1005/2010, (UE) n. 1008/2010, (UE) n. 1009/2010, (UE) n. 19/2011, (UE) n. 109/2011, (UE) n. 458/2011, (UE) n. 65/2012, (UE) n. 130/2012, (UE) n. 347/2012, (UE) n. 351/2012, (UE) n. 1230/2012 e (UE) 2015/166 (GU L 325 del 16.12.2019, pag. 1).

cibersicurezza[11] e prevedendo specifiche procedure di valutazione della conformità. Nel settore dell'aviazione, il regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio[12] ha come obiettivo principale stabilire e mantenere un livello elevato ed uniforme di sicurezza dell'aviazione civile nell'Unione. Esso istituisce un quadro di requisiti essenziali per l'aeronavigabilità di prodotti aeronautici, parti ed equipaggiamenti, compreso il software, che tengono conto degli obblighi di protezione dalle minacce alla *security* delle informazioni. I prodotti con elementi digitali a cui si applica il regolamento (UE) 2019/2144 e quelli certificati in conformità del regolamento (UE) 2018/1139 non sono pertanto soggetti ai requisiti essenziali e alle procedure di valutazione della conformità di cui al presente regolamento. Il processo di certificazione a norma del regolamento (UE) 2018/1139 assicura il livello di garanzia perseguito dal presente regolamento.

(14) Il presente regolamento stabilisce norme orizzontali in materia di cibersicurezza che non sono specifiche per settori o per determinati prodotti con elementi digitali. Tuttavia potrebbero essere introdotte norme dell'Unione settoriali o specifiche per prodotto, volte a stabilire requisiti che affrontano tutti o alcuni rischi coperti dai requisiti essenziali stabiliti dal presente regolamento. In tali casi l'applicazione del presente regolamento ai prodotti con elementi digitali contemplati da altre norme dell'Unione, che stabiliscono requisiti che affrontano tutti o alcuni rischi coperti dai requisiti essenziali di cui all'allegato I del presente regolamento, può essere limitata o esclusa, qualora tale limitazione o esclusione sia coerente con il quadro normativo generale applicabile a tali prodotti e qualora le norme settoriali conseguano lo stesso livello di protezione previsto dal presente regolamento. Alla Commissione è conferito il potere di adottare atti delegati per modificare il presente regolamento individuando tali prodotti e norme. Per quanto riguarda la normativa dell'Unione vigente in cui dovrebbero essere applicate tali limitazioni o esclusioni, il presente regolamento contiene disposizioni specifiche per chiarire il suo rapporto con tale normativa dell'Unione.

(15) Il regolamento delegato (UE) 2022/30 specifica che i requisiti essenziali di cui all'articolo 3, paragrafo 3, lettera d) (danni alla rete e abuso delle risorse della rete), lettera e) (dati personali e vita privata) e lettera f) (frodi) della direttiva 2014/53/UE si applicano a determinate apparecchiature radio. La [decisione di esecuzione XXX/2022 della Commissione relativa ad una richiesta di normazione rivolta alle organizzazioni europee di normazione] stabilisce i requisiti per l'elaborazione di norme specifiche, precisando inoltre il modo in cui dovrebbero essere trattati questi tre requisiti essenziali. I requisiti essenziali stabiliti dal presente regolamento comprendono tutti gli elementi dei requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere d), e) e f), della direttiva 2014/53/UE. I requisiti essenziali stabiliti nel presente regolamento sono inoltre allineati con gli obiettivi dei requisiti delle norme specifiche incluse in tale richiesta di normazione. Pertanto, se la Commissione abroga o modifica il

---

[11] Regolamento n. 155 della Commissione economica per l'Europa delle Nazioni Unite (UNECE) – Disposizioni uniformi relative all'omologazione dei veicoli per quanto riguarda la cibersicurezza e i sistemi di gestione della cibersicurezza [2021/387].

[12] 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 e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio (GU L 212 del 22.8.2018, pag. 1).

regolamento delegato (UE) 2022/30, con la conseguenza che esso cessa di applicarsi a determinati prodotti soggetti al presente regolamento, la Commissione e le organizzazioni europee di normazione dovrebbero tenere conto dei lavori di normazione svolti nel contesto della decisione di esecuzione C(2022)5637 della Commissione relativa ad una richiesta di normazione per il regolamento delegato (UE) 2022/30 che integra la direttiva sulle apparecchiature radio nella preparazione e nello sviluppo di norme armonizzate per facilitare l'attuazione del presente regolamento.

(16) La direttiva 85/374/CEE[13] è complementare al presente regolamento. Tale direttiva stabilisce le norme in materia di responsabilità per danno da prodotti difettosi, in modo che i danneggiati possano chiedere il risarcimento quando un danno è stato causato da prodotti difettosi. Essa stabilisce il principio secondo cui il fabbricante di un prodotto è responsabile dei danni causati da una mancanza di sicurezza nel suo prodotto indipendentemente dalla colpa ("responsabilità oggettiva"). Se tale mancanza di sicurezza consiste nell'assenza di aggiornamenti di sicurezza dopo l'immissione sul mercato del prodotto e ciò causa un danno, questo potrebbe far scattare la responsabilità del fabbricante. Gli obblighi dei fabbricanti relativi alla fornitura di tali aggiornamenti di sicurezza dovrebbero essere stabiliti nel presente regolamento.

(17) Il presente regolamento dovrebbe lasciare impregiudicato il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[14], comprese le disposizioni per l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità a detto regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Tali operazioni potrebbero essere integrate in un prodotto con elementi digitali. La protezione dei dati fin dalla progettazione e per impostazione predefinita e la cibersicurezza in generale sono elementi fondamentali del regolamento (UE) 2016/679. Proteggendo i consumatori e le organizzazioni dai rischi di cibersicurezza, i requisiti essenziali di cibersicurezza stabiliti nel presente regolamento dovrebbero inoltre contribuire a migliorare la protezione dei dati personali e della vita privata delle persone. Dovrebbero essere considerate le sinergie sia nell'ambito della normazione che della certificazione relativamente agli aspetti di cibersicurezza attraverso la cooperazione tra la Commissione, le organizzazioni europee di normazione, l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), il comitato europeo per la protezione dei dati (EDPB) istituito dal regolamento (UE) 2016/679 e le autorità nazionali di controllo della protezione dei dati. È opportuno creare sinergie tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati anche nel settore della vigilanza del mercato e dell'applicazione della normativa. A tal fine le autorità nazionali di vigilanza del mercato nominate a norma del presente regolamento dovrebbero cooperare con le autorità preposte alla vigilanza del diritto dell'Unione in materia di protezione dei dati. Queste ultime dovrebbero inoltre avere accesso alle informazioni pertinenti per lo svolgimento dei loro compiti.

---

13 Direttiva 85/374/CEE del Consiglio, del 25 luglio 1985, relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi (GU L 210 del 7.8.1985, pag. 29).

14 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

(18) Nella misura in cui i loro prodotti rientrano nell'ambito di applicazione del presente regolamento, gli emittenti dei portafogli europei di identità digitale di cui all'articolo [articolo 6 bis, paragrafo 2, del regolamento (UE) n. 910/2014, modificato dalla proposta di regolamento che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea] dovrebbero essere conformi sia ai requisiti essenziali orizzontali stabiliti dal presente regolamento sia ai requisiti di sicurezza specifici stabiliti dall'articolo [articolo 6 bis del regolamento (UE) n. 910/2014, modificato dalla proposta di regolamento che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea]. Al fine di facilitare la conformità, gli emittenti dei portafogli dovrebbero poter dimostrare la conformità dei portafogli europei di identità digitale ai requisiti stabiliti in ciascuno dei due atti certificando i loro prodotti nell'ambito di un sistema europeo di certificazione della cibersicurezza istituito a norma del regolamento (UE) 2019/881 e per il quale la Commissione ha specificato, mediante atto di esecuzione, una presunzione di conformità al presente regolamento, nella misura in cui il certificato o sue parti contemplino tali requisiti.

(19) Alcuni compiti previsti dal presente regolamento dovrebbero essere svolti dall'ENISA, conformemente all'articolo 3, paragrafo 2, del regolamento (UE) 2019/881. In particolare l'ENISA dovrebbe ricevere le notifiche dei fabbricanti relative alle vulnerabilità attivamente sfruttate contenute nei prodotti con elementi digitali, nonché agli incidenti che hanno un impatto sulla sicurezza di tali prodotti. L'ENISA dovrebbe inoltre trasmettere tali notifiche ai pertinenti gruppi di intervento per la sicurezza informatica in caso di incidente (*Computer Security Incident Response Teams* – CSIRT) o ai pertinenti punti di contatto unici degli Stati membri designati conformemente all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)] e informare le autorità di vigilanza del mercato competenti in merito alla vulnerabilità notificata. Sulla base delle informazioni raccolte, l'ENISA dovrebbe preparare una relazione tecnica biennale sulle tendenze emergenti relative ai rischi di cibersicurezza nei prodotti con elementi digitali e presentarla al gruppo di cooperazione di cui alla direttiva [direttiva XXX/XXXX (NIS2)]. Inoltre, considerando le sue competenze e il suo mandato, l'ENISA dovrebbe poter sostenere il processo di attuazione del presente regolamento. In particolare dovrebbe poter proporre attività congiunte che saranno svolte dalle autorità di vigilanza del mercato sulla base di indicazioni o informazioni riguardanti la potenziale non conformità al presente regolamento di prodotti con elementi digitali in diversi Stati membri o di individuare categorie di prodotti per le quali dovrebbero essere organizzate azioni di controllo coordinate e simultanee. In circostanze eccezionali, su richiesta della Commissione, l'ENISA dovrebbe poter effettuare valutazioni su specifici prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo, qualora sia necessario un intervento immediato per preservare il buon funzionamento del mercato interno.

(20) I prodotti con elementi digitali dovrebbero recare la marcatura CE per indicare la loro conformità al presente regolamento, in modo da poter circolare liberamente nel mercato interno. Gli Stati membri non dovrebbero ostacolare in maniera ingiustificata l'immissione sul mercato di prodotti con elementi digitali che soddisfano i requisiti stabiliti nel presente regolamento e che recano la marcatura CE.

(21) Per far sì che i fabbricanti possano rilasciare software ai fini di prova prima di sottoporre i loro prodotti alla valutazione della conformità, gli Stati membri non dovrebbero impedire la messa a disposizione di software non finiti, come versioni alfa, versioni beta o *release candidate*, a condizione che la versione sia messa a

disposizione solo per il tempo necessario a testarla e a raccogliere riscontri. I fabbricanti dovrebbero provvedere affinché il software messo a disposizione a tali condizioni sia rilasciato solo a seguito di una valutazione dei rischi e sia conforme, per quanto possibile, ai requisiti di sicurezza relativi alle proprietà dei prodotti con elementi digitali imposti dal presente regolamento. I fabbricanti dovrebbero inoltre attuare, nella misura del possibile, i requisiti di gestione delle vulnerabilità. I fabbricanti non dovrebbero costringere gli utilizzatori a passare alle versioni rilasciate solo ai fini di prova.

(22) Per garantire che i prodotti con elementi digitali, quando sono immessi sul mercato, non presentino rischi di cibersicurezza per le persone e le organizzazioni, è opportuno stabilire requisiti essenziali per tali prodotti. Qualora i prodotti vengano successivamente modificati, da mezzi fisici o digitali, in un modo non previsto dal fabbricante e che potrebbe implicare il fatto che essi non rispettino più i requisiti essenziali pertinenti, la modifica dovrebbe essere considerata sostanziale. Ad esempio gli aggiornamenti o le riparazioni del software potrebbero essere assimilati a interventi di manutenzione purché non modifichino un prodotto già immesso sul mercato in maniera tale da poter influire sulla sua conformità ai requisiti applicabili o da modificare l'uso previsto per il quale il prodotto è stato valutato. Come avviene per le modifiche o le riparazioni fisiche, un prodotto con elementi digitali dovrebbe essere considerato modificato sostanzialmente da un cambiamento del software qualora l'aggiornamento del software modifichi le funzioni, il tipo o le prestazioni originari del prodotto e ciò non fosse previsto nella valutazione dei rischi iniziale, o qualora la natura del pericolo sia cambiata o il livello di rischio sia aumentato a causa dell'aggiornamento del software.

(23) In linea con la nozione generalmente riconosciuta di modifica sostanziale dei prodotti disciplinati dalla normativa di armonizzazione dell'Unione, ogniqualvolta intervenga una modifica sostanziale che possa incidere sulla conformità di un prodotto al presente regolamento oppure quando venga modificata la sua finalità prevista, è opportuno verificare la conformità del prodotto con elementi digitali e sottoporlo, se del caso, a una nuova valutazione della conformità. Ove applicabile, se il fabbricante effettua una valutazione della conformità che coinvolge terzi, i cambiamenti che potrebbero comportare modifiche sostanziali dovrebbero essere notificati a questi ultimi.

(24) Il ricondizionamento, la manutenzione e la riparazione di un prodotto con elementi digitali, come definiti nel regolamento [regolamento sulla progettazione ecocompatibile], non comportano necessariamente una modifica sostanziale del prodotto, ad esempio se l'uso e le funzionalità previsti non sono modificati e il livello di rischio rimane inalterato. Tuttavia il miglioramento di un prodotto da parte del fabbricante potrebbe comportare modifiche nella progettazione e nello sviluppo del prodotto stesso e quindi influire sull'uso previsto e sulla conformità del prodotto ai requisiti stabiliti nel presente regolamento.

(25) I prodotti con elementi digitali dovrebbero essere considerati critici se lo sfruttamento di potenziali vulnerabilità di cibersicurezza nel prodotto può provocare un impatto negativo grave a causa, tra l'altro, della funzionalità legata alla cibersicurezza o dell'uso previsto. In particolare le vulnerabilità nei prodotti con elementi digitali dotati di una funzionalità legata alla cibersicurezza, come gli elementi sicuri, possono determinare una propagazione dei problemi di sicurezza lungo l'intera catena di approvvigionamento. La gravità dell'impatto di un incidente di cibersicurezza può anche aumentare se si tiene conto dell'uso previsto del prodotto, ad esempio in un ambiente industriale o nel contesto di un soggetto essenziale del tipo di cui all'allegato

[allegato I] della direttiva [direttiva XXX/XXXX (NIS2)], o se si svolgono funzioni critiche o sensibili, come il trattamento dei dati personali.

(26) I prodotti con elementi digitali critici dovrebbero essere soggetti a procedure di valutazione della conformità più rigorose, pur mantenendo un approccio proporzionato. A tal fine i prodotti con elementi digitali critici dovrebbero essere suddivisi in due classi che riflettono il livello di rischio di cibersicurezza legato a tali categorie di prodotti. Un potenziale incidente informatico che coinvolga prodotti di classe II potrebbe avere impatti negativi maggiori rispetto a un incidente che coinvolga prodotti di classe I, ad esempio a causa della natura della loro funzione legata alla cibersicurezza o dell'uso previsto in ambienti sensibili, e pertanto dovrebbero essere sottoposti a una procedura di valutazione della conformità più rigorosa.

(27) Le categorie di prodotti con elementi digitali critici di cui all'allegato III del presente regolamento dovrebbero essere intese come prodotti la cui funzionalità principale è del tipo indicato al medesimo allegato. L'allegato III del presente regolamento elenca ad esempio i prodotti che, in base alla loro funzionalità principale, sono definiti microprocessori di uso generale di classe II. Di conseguenza questi ultimi sono soggetti a una valutazione della conformità obbligatoria da parte di terzi. Ciò non si applica ad altri prodotti non esplicitamente menzionati nell'allegato III del presente regolamento che possono integrare un microprocessore di uso generale. La Commissione dovrebbe adottare atti delegati [entro 12 mesi dall'entrata in vigore del presente regolamento] per precisare le definizioni delle categorie di prodotti rientranti nelle classi I e II di cui all'allegato III.

(28) Il presente regolamento affronta i rischi di cibersicurezza in modo mirato. I prodotti con elementi digitali possono tuttavia comportare altri rischi di sicurezza che non sono connessi alla cibersicurezza. Tali rischi dovrebbero continuare a essere regolamentati da altre normative dell'Unione pertinenti in materia di prodotti. Se non sono applicabili altre normative di armonizzazione dell'Unione, essi dovrebbero essere soggetti al regolamento [regolamento relativo alla sicurezza generale dei prodotti]. Pertanto, alla luce della natura mirata del presente regolamento, in deroga all'articolo 2, paragrafo 1, terzo comma, lettera b), del regolamento [regolamento relativo alla sicurezza generale dei prodotti], il capo III, sezione 1, i capi V e VII e i capi da IX a XI del regolamento [regolamento relativo alla sicurezza generale dei prodotti] dovrebbero applicarsi ai prodotti con elementi digitali per quanto riguarda i rischi di sicurezza non contemplati dal presente regolamento, qualora tali prodotti non siano soggetti a requisiti specifici imposti da altre normative di armonizzazione dell'Unione ai sensi dell'[articolo 3, punto 25, del regolamento relativo alla sicurezza generale dei prodotti].

(29) I prodotti con elementi digitali classificati come sistemi di IA ad alto rischio conformemente all'articolo 6 del regolamento[15] [regolamento sull'IA] che rientrano nell'ambito di applicazione del presente regolamento dovrebbero essere conformi ai requisiti essenziali stabiliti da quest'ultimo. Quando soddisfano i requisiti essenziali del presente regolamento, tali sistemi di IA ad alto rischio dovrebbero presumersi conformi ai requisiti di cibersicurezza di cui all'articolo [articolo 15] del regolamento [regolamento sull'IA] nella misura in cui tali requisiti siano contemplati dalla dichiarazione di conformità UE, o da sue parti, rilasciata a norma del presente regolamento. Per quanto riguarda le procedure di valutazione della conformità relative ai requisiti essenziali di cibersicurezza di un prodotto con elementi digitali

[15] Regolamento [regolamento sull'IA].

contemplato dal presente regolamento e classificato come sistema di IA ad alto rischio, è opportuno che si applichino come norma generale le disposizioni pertinenti dell'articolo 43 del regolamento [regolamento sull'IA] anziché le rispettive disposizioni del presente regolamento. Tuttavia tale norma non dovrebbe comportare una riduzione del livello di garanzia necessario per i prodotti con elementi digitali critici contemplati dal presente regolamento. Pertanto, in deroga a detta norma, i sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del regolamento [regolamento sull'IA] e che sono anche qualificati come prodotti con elementi digitali critici a norma del presente regolamento e ai quali si applica la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI del regolamento [regolamento sull'IA] dovrebbero essere soggetti alle disposizioni in materia di valutazione della conformità del presente regolamento per quanto riguarda i requisiti essenziali dello stesso. In questo caso, per tutti gli altri aspetti contemplati dal regolamento [regolamento sull'AI], è opportuno applicare le rispettive disposizioni in materia di valutazione della conformità basata sul controllo interno di cui all'allegato VI del regolamento [regolamento sull'IA].

(30) I prodotti macchina che rientrano nell'ambito di applicazione del regolamento [proposta di regolamento sui prodotti macchina] che sono prodotti con elementi digitali ai sensi del presente regolamento e per i quali è stata rilasciata una dichiarazione di conformità sulla base di quest'ultimo dovrebbero presumersi conformi ai requisiti essenziali di sicurezza e di tutela della salute di cui all'[allegato III, sezioni 1.1.9 e 1.2.1] del regolamento [proposta di regolamento sui prodotti macchina], per quanto concerne la protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo nella misura in cui la conformità a tali requisiti sia dimostrata dalla dichiarazione di conformità UE rilasciata a norma del presente regolamento.

(31) Il regolamento [proposta di regolamento sullo spazio europeo dei dati sanitari] integra i requisiti essenziali stabiliti dal presente regolamento. I sistemi di cartelle cliniche elettroniche che rientrano nell'ambito di applicazione del regolamento [proposta di regolamento sullo spazio europeo dei dati sanitari] e che sono prodotti con elementi digitali ai sensi del presente regolamento dovrebbero pertanto essere conformi ai requisiti essenziali stabiliti da quest'ultimo. I fabbricanti dovrebbero dimostrare la conformità dei loro sistemi secondo quanto disposto dal regolamento [proposta di regolamento sullo spazio europeo dei dati sanitari]. Per facilitare la conformità, i fabbricanti possono redigere un'unica documentazione tecnica contenente gli elementi richiesti da entrambi gli atti giuridici. Poiché il presente regolamento non riguarda il SaaS in quanto tale, i sistemi di cartelle cliniche elettroniche offerti attraverso il modello di licenza e fornitura SaaS non rientrano nell'ambito di applicazione del presente regolamento. Analogamente i sistemi di cartelle cliniche elettroniche sviluppati e utilizzati internamente non rientrano nell'ambito di applicazione del presente regolamento, in quanto non sono immessi sul mercato.

(32) Al fine di garantire che i prodotti con elementi digitali siano sicuri sia al momento dell'immissione sul mercato sia durante l'intero ciclo di vita, è necessario stabilire requisiti essenziali per la gestione delle vulnerabilità e requisiti essenziali di cibersicurezza relativi alle proprietà dei prodotti con elementi digitali. Se da un lato i fabbricanti dovrebbero soddisfare tutti i requisiti essenziali relativi alla gestione delle vulnerabilità e garantire che tutti i loro prodotti siano consegnati senza vulnerabilità note sfruttabili, dall'altro dovrebbero determinare quali altri requisiti essenziali relativi alle proprietà del prodotto sono pertinenti per il tipo di prodotto in questione. A tal fine è opportuno che i fabbricanti effettuino una valutazione dei rischi di cibersicurezza

associati a un prodotto con elementi digitali per identificare i rischi e i requisiti essenziali pertinenti e per applicare in modo appropriato le norme armonizzate o le specifiche comuni adeguate.

(33) Per migliorare la sicurezza dei prodotti con elementi digitali immessi sul mercato interno occorre stabilire requisiti essenziali. Tali requisiti essenziali non dovrebbero pregiudicare le valutazioni dei rischi coordinate a livello dell'UE delle catene di approvvigionamento critiche stabilite dall'[articolo X] della direttiva [direttiva XXX/XXXX (NIS2)][16], che tengono conto sia dei fattori di rischio tecnici sia, se pertinente, di quelli non tecnici, come l'indebita influenza di un paese terzo sui fornitori. Inoltre ciò non dovrebbe pregiudicare le prerogative degli Stati membri di stabilire requisiti aggiuntivi che tengano conto di fattori non tecnici al fine di garantire un livello elevato di resilienza, compresi quelli definiti nella raccomandazione (UE) 2019/534, nella valutazione dei rischi coordinata a livello dell'UE della sicurezza delle reti 5G e nel pacchetto di strumenti dell'UE sulla cibersicurezza del 5G concordato dal gruppo di cooperazione NIS di cui alla [direttiva XXX/XXXX (NIS2)].

(34) Per garantire che i CSIRT nazionali e i punti di contatto unici designati conformemente all'articolo [articolo X] della direttiva [direttiva XX/XXXX (NIS2)] ricevano le informazioni necessarie per svolgere i loro compiti e innalzare il livello generale di cibersicurezza dei soggetti essenziali e importanti e per garantire il funzionamento efficace delle autorità di vigilanza del mercato, i fabbricanti di prodotti con elementi digitali dovrebbero notificare all'ENISA le vulnerabilità attivamente sfruttate. Poiché la maggior parte dei prodotti con elementi digitali è commercializzata sull'intero mercato interno, qualsiasi vulnerabilità sfruttata in un prodotto con elementi digitali dovrebbe essere considerata una minaccia al funzionamento del mercato interno. I fabbricanti dovrebbero inoltre considerare la possibilità di divulgare le vulnerabilità risolte alla banca dati europea delle vulnerabilità istituita a norma della direttiva [direttiva XX/XXXX (NIS2)] e gestita dall'ENISA o a qualsiasi altra banca dati delle vulnerabilità accessibile al pubblico.

(35) I fabbricanti dovrebbero anche segnalare all'ENISA qualsiasi incidente che abbia un impatto sulla sicurezza del prodotto con elementi digitali. Fatti salvi gli obblighi di segnalazione degli incidenti previsti dalla direttiva [direttiva XXX/XXXX (NIS2)] per i soggetti essenziali e importanti, è fondamentale che l'ENISA, i punti di contatto unici designati dagli Stati membri conformemente all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)] e le autorità di vigilanza del mercato ricevano informazioni dai fabbricanti di prodotti con elementi digitali che consentano loro di valutare la sicurezza di tali prodotti. Per far sì che gli utilizzatori possano reagire rapidamente agli incidenti che hanno un impatto sulla sicurezza dei loro prodotti con elementi digitali, i fabbricanti dovrebbero inoltre informare gli utilizzatori di tali incidenti e, se del caso, di eventuali misure correttive che gli utilizzatori potrebbero adottare per attenuarne l'impatto, ad esempio attraverso la pubblicazione di informazioni pertinenti sui propri siti web o il contatto diretto, qualora il fabbricante sia in grado di contattare gli utilizzatori e ciò sia giustificato dai rischi.

(36) I fabbricanti di prodotti con elementi digitali dovrebbero mettere in atto politiche di divulgazione coordinata delle vulnerabilità per facilitare la segnalazione delle

[16] Direttiva XXX del Parlamento europeo e del Consiglio, del [data], [relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (GU L xx del [data], pag. x)].

vulnerabilità da parte di individui o soggetti. Una politica di divulgazione coordinata delle vulnerabilità dovrebbe indicare un processo strutturato attraverso il quale le vulnerabilità sono segnalate al fabbricante in modo da consentire a quest'ultimo di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano comunicate a terzi o al pubblico. Dato che le informazioni sulle vulnerabilità sfruttabili in prodotti con elementi digitali di largo consumo possono essere vendute a prezzi elevati sul mercato nero, i fabbricanti di tali prodotti, nell'ambito delle loro politiche di divulgazione coordinata delle vulnerabilità, dovrebbero poter utilizzare programmi volti a incentivare la segnalazione delle vulnerabilità garantendo che individui o soggetti ricevano un riconoscimento e un compenso per i loro sforzi (i cosiddetti "programmi di bug bounty").

(37) Per facilitare l'analisi delle vulnerabilità, i fabbricanti dovrebbero individuare e documentare i componenti contenuti nei prodotti con elementi digitali, creando anche una distinta base del software. Tale distinta può fornire a coloro che realizzano, acquistano e utilizzano il software informazioni che migliorano la loro comprensione della catena di approvvigionamento, con molteplici vantaggi, in particolare quello di aiutare i fabbricanti e gli utilizzatori a tenere traccia delle vulnerabilità e dei rischi noti emersi di recente. È particolarmente importante che i fabbricanti garantiscano che i loro prodotti non contengono componenti vulnerabili sviluppati da terzi.

(38) Al fine di facilitare la valutazione della conformità ai requisiti stabiliti dal presente regolamento, è opportuno che vi sia una presunzione di conformità per i prodotti con elementi digitali conformi alle norme armonizzate che traducono i requisiti essenziali del presente regolamento in specifiche tecniche dettagliate e che sono adottate conformemente al regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio[17]. Il regolamento (UE) n. 1025/2012 prevede una procedura di obiezione a norme armonizzate che non soddisfano completamente i requisiti del presente regolamento.

(39) Il regolamento (UE) 2019/881 istituisce un quadro volontario europeo di certificazione della cibersicurezza per i prodotti, i servizi e i processi TIC. I sistemi europei di certificazione della cibersicurezza possono applicarsi ai prodotti con elementi digitali contemplati dal presente regolamento. Il presente regolamento dovrebbe creare sinergie con il regolamento (UE) 2019/881. Al fine di facilitare la valutazione della conformità ai requisiti stabiliti nel presente regolamento, i prodotti con elementi digitali che sono certificati o per i quali è stata rilasciata una dichiarazione di conformità nell'ambito di un sistema di cibersicurezza a norma del regolamento (UE) 2019/881 e identificato dalla Commissione in un atto di esecuzione sono considerati conformi ai requisiti essenziali del presente regolamento nella misura in cui tali requisiti siano contemplati nel certificato di cibersicurezza o nella dichiarazione di conformità o in parti di essi. La necessità di nuovi sistemi europei di certificazione della cibersicurezza per i prodotti con elementi digitali dovrebbe essere valutata alla luce del presente regolamento. Tali futuri sistemi europei di certificazione della cibersicurezza relativi ai prodotti con elementi digitali dovrebbero tenere conto dei

[17] Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

requisiti essenziali stabiliti nel presente regolamento e facilitare la conformità a quest'ultimo. Alla Commissione dovrebbe essere conferito il potere di specificare, mediante atti di esecuzione, i sistemi europei di certificazione della cibersicurezza che possono essere utilizzati per dimostrare la conformità ai requisiti essenziali stabiliti nel presente regolamento. Inoltre, al fine di evitare un onere amministrativo indebito a carico dei fabbricanti, la Commissione dovrebbe specificare, ove applicabile, se un certificato di cibersicurezza rilasciato nell'ambito di tali sistemi europei di certificazione della cibersicurezza sopprime l'obbligo per i fabbricanti di effettuare una valutazione della conformità da parte di terzi, come previsto dal presente regolamento per i requisiti corrispondenti.

(40) All'entrata in vigore dell'atto di esecuzione che istituisce il [regolamento di esecuzione (UE) .../... della Commissione, del XXX, sul sistema europeo di certificazione della cibersicurezza basato sui criteri comuni], che riguarda i prodotti hardware contemplati dal presente regolamento, come i microprocessori e i moduli di sicurezza dell'hardware, la Commissione può specificare, mediante atto di esecuzione, come tale sistema conferisca una presunzione di conformità ai requisiti essenziali di cui all'allegato I del presente regolamento o a loro parti. Inoltre tale atto di esecuzione può specificare in che modo un certificato rilasciato nell'ambito del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni sopprima l'obbligo per i fabbricanti di effettuare una valutazione da parte di terzi, come previsto dal presente regolamento per i requisiti corrispondenti.

(41) Se non sono adottate norme armonizzate o se le norme armonizzate non affrontano in misura sufficiente i requisiti essenziali del presente regolamento, la Commissione dovrebbe poter adottare specifiche comuni mediante atti di esecuzione. Tra le ragioni per definire tali specifiche comuni, anziché utilizzare norme armonizzate, possono figurare il rifiuto della richiesta di normazione da parte di una qualsiasi organizzazione europea di normazione, ritardi ingiustificati nell'elaborazione di norme armonizzate appropriate o la mancanza di conformità delle norme elaborate ai requisiti del presente regolamento o a una richiesta della Commissione. Per facilitare la valutazione della conformità ai requisiti essenziali stabiliti dal presente regolamento, è opportuno che vi sia una presunzione di conformità per i prodotti con elementi digitali conformi alle specifiche comuni adottate dalla Commissione a norma del presente regolamento al fine della formulazione di specifiche tecniche dettagliate in relazione a tali requisiti.

(42) I fabbricanti dovrebbero redigere una dichiarazione di conformità UE che fornisca le informazioni richieste a norma del presente regolamento sulla conformità dei prodotti con elementi digitali ai requisiti essenziali stabiliti dal presente regolamento e, ove applicabile, da altri atti pertinenti della normativa di armonizzazione dell'Unione che disciplinano tale prodotto. I fabbricanti possono altresì essere tenuti a redigere una dichiarazione di conformità UE in base a un'altra normativa dell'Unione. Al fine di garantire un accesso efficace alle informazioni per fini di vigilanza del mercato, dovrebbe essere redatta un'unica dichiarazione di conformità UE per quanto riguarda la conformità a tutti gli atti pertinenti dell'Unione. Al fine di ridurre l'onere amministrativo a carico degli operatori economici, tale dichiarazione di conformità UE unica dovrebbe poter consistere in un fascicolo comprendente le dichiarazioni di conformità individuali pertinenti.

(43) La marcatura CE, che indica la conformità di un prodotto, è la conseguenza visibile di un intero processo che comprende la valutazione della conformità in senso lato. I

principi generali che disciplinano la marcatura CE sono indicati nel regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio[18]. È opportuno che nel presente regolamento siano fissate le norme relative all'apposizione della marcatura CE sui prodotti con elementi digitali. La marcatura CE dovrebbe essere l'unica marcatura che garantisce la conformità dei prodotti con elementi digitali ai requisiti del presente regolamento.

(44) Per consentire agli operatori economici di dimostrare la conformità ai requisiti essenziali stabiliti nel presente regolamento e alle autorità di vigilanza del mercato di garantire che i prodotti con elementi digitali messi a disposizione sul mercato siano conformi a tali requisiti, è necessario prevedere procedure di valutazione della conformità. La decisione n. 768/2008/CE del Parlamento europeo e del Consiglio[19] stabilisce moduli per le procedure di valutazione della conformità proporzionalmente al livello di rischio effettivo e di sicurezza richiesto. Per garantire la coerenza intersettoriale ed evitare varianti ad hoc, le procedure di valutazione della conformità adeguate per verificare la conformità dei prodotti con elementi digitali ai requisiti essenziali stabiliti nel presente regolamento sono basate su tali moduli. Le procedure di valutazione della conformità dovrebbero esaminare e verificare sia i requisiti relativi al prodotto sia quelli relativi al processo riguardanti l'intero ciclo di vita dei prodotti con elementi digitali, tra cui la pianificazione, la progettazione, lo sviluppo o la produzione, il collaudo e la manutenzione del prodotto.

(45) La valutazione della conformità dei prodotti con elementi digitali dovrebbe essere di norma effettuata dal fabbricante sotto la propria responsabilità, applicando la procedura basata sul modulo A della decisione n. 768/2008/CE. Il fabbricante dovrebbe mantenere la flessibilità di scegliere una procedura di valutazione della conformità più rigorosa che coinvolga terzi. Se il prodotto è classificato come prodotto critico di classe I, è necessaria una garanzia supplementare per dimostrare la conformità ai requisiti essenziali stabiliti nel presente regolamento. Se intende effettuare la valutazione della conformità sotto la propria responsabilità (modulo A), il fabbricante dovrebbe applicare le norme armonizzate, le specifiche comuni o i sistemi di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881 che sono stati identificati dalla Commissione in un atto di esecuzione. Se non applica tali norme armonizzate, specifiche comuni o sistemi di certificazione della cibersicurezza, il fabbricante dovrebbe effettuare una valutazione della conformità che coinvolga terzi. Tenendo conto dell'onere amministrativo a carico dei fabbricanti e del fatto che la cibersicurezza svolge un ruolo importante nella fase di progettazione e sviluppo dei prodotti tangibili e intangibili con elementi digitali, le procedure di valutazione della conformità basate rispettivamente sui moduli B+C o sul modulo H della decisione 768/2008/CE sono state scelte come le più appropriate per valutare la conformità dei prodotti con elementi digitali critici in modo proporzionato ed efficace. Il fabbricante che effettua la valutazione della conformità da parte di terzi può scegliere la procedura che meglio si adatta al suo processo di progettazione e produzione. Dato il rischio di cibersicurezza ancora maggiore legato all'uso di prodotti classificati come prodotti critici di classe II, la valutazione della conformità dovrebbe sempre coinvolgere terzi.

---

[18] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che fissa le norme in materia di accreditamento e abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

[19] Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE (GU L 218 del 13.8.2008, pag. 82).

(46) Mentre la creazione di prodotti tangibili con elementi digitali richiede di norma un notevole impegno da parte dei fabbricanti nelle fasi di progettazione, sviluppo e produzione, la creazione di prodotti con elementi digitali sotto forma di software si concentra quasi esclusivamente sulla progettazione e sullo sviluppo, mentre la fase di produzione svolge un ruolo minore. Tuttavia in molti casi i prodotti software devono ancora essere compilati, costruiti, pacchettizzati, messi a disposizione per il download o copiati su supporti fisici prima di essere immessi sul mercato. Tali attività dovrebbero essere considerate attività assimilabili alla produzione quando si applicano i moduli di valutazione della conformità pertinenti per verificare la conformità del prodotto ai requisiti essenziali del presente regolamento nelle fasi di progettazione, sviluppo e produzione.

(47) Ai fini della valutazione della conformità da parte di terzi dei prodotti con elementi digitali, le autorità nazionali di notifica dovrebbero notificare gli organismi di valutazione della conformità alla Commissione e agli altri Stati membri, a condizione che tali organismi soddisfino una serie di requisiti, in particolare in materia di indipendenza, competenza e assenza di conflitti di interesse.

(48) Per garantire un livello uniforme di qualità nello svolgimento della valutazione della conformità dei prodotti con elementi digitali, è altresì necessario stabilire requisiti da applicare alle autorità di notifica e agli altri organismi che intervengono nella valutazione, nella notifica e nel controllo degli organismi notificati. Il sistema previsto dal presente regolamento dovrebbe essere completato dal sistema di accreditamento di cui al regolamento (CE) n. 765/2008. Poiché l'accreditamento è un mezzo essenziale per la verifica della competenza degli organismi di valutazione della conformità, è opportuno impiegarlo anche ai fini della notifica.

(49) L'accreditamento trasparente, quale previsto dal regolamento (CE) n. 765/2008, che garantisce il necessario livello di fiducia nei certificati di conformità, dovrebbe essere considerato dalle autorità pubbliche nazionali in tutta l'Unione lo strumento preferito per dimostrare la competenza tecnica di tali organismi. Tuttavia le autorità nazionali possono ritenere di possedere gli strumenti idonei a eseguire da sé tale valutazione. In tal caso, onde assicurare l'opportuno livello di credibilità delle valutazioni effettuate dalle altre autorità nazionali, dovrebbero fornire alla Commissione e agli altri Stati membri le necessarie prove documentali che dimostrino che gli organismi di valutazione della conformità valutati rispettano le pertinenti prescrizioni regolamentari.

(50) Spesso gli organismi di valutazione della conformità subappaltano parti delle loro attività connesse alla valutazione della conformità o fanno ricorso ad un'affiliata. Al fine di salvaguardare il livello di tutela richiesto per il prodotto con elementi digitali da immettere sul mercato, è indispensabile che i subappaltatori e le affiliate di valutazione della conformità rispettino gli stessi requisiti applicati agli organismi notificati in relazione allo svolgimento di compiti di valutazione della conformità.

(51) La notifica di un organismo di valutazione della conformità dovrebbe essere inviata dall'autorità di notifica alla Commissione e agli altri Stati membri tramite il sistema informativo NANDO (*New Approach Notified and Designated Organisations*). NANDO è lo strumento elettronico di notifica elaborato e gestito dalla Commissione in cui è possibile trovare un elenco di tutti gli organismi notificati.

(52) Poiché gli organismi notificati possono offrire i propri servizi in tutta l'Unione, è opportuno conferire agli altri Stati membri e alla Commissione la possibilità di sollevare obiezioni relative a un organismo notificato. È pertanto importante prevedere

un periodo durante il quale sia possibile chiarire eventuali dubbi o preoccupazioni circa la competenza degli organismi di valutazione della conformità prima che essi inizino ad operare in qualità di organismi notificati.

(53) Nell'interesse della competitività, è fondamentale che gli organismi notificati applichino le procedure di valutazione della conformità senza creare un onere superfluo per gli operatori economici. Analogamente, e per garantire parità di trattamento agli operatori economici dovrebbe essere garantita un'applicazione tecnica coerente delle procedure di valutazione della conformità. Essa dovrebbe essere ottenuta più agevolmente mediante un coordinamento e una cooperazione appropriati tra organismi notificati.

(54) La vigilanza del mercato è un'attività essenziale per garantire l'applicazione corretta ed uniforme della normativa dell'Unione. Di conseguenza è opportuno istituire un quadro giuridico entro il quale la vigilanza del mercato possa svolgersi in maniera adeguata. Le norme sulla vigilanza del mercato dell'Unione e sul controllo dei prodotti che entrano nel mercato dell'Unione di cui al regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio[20] si applicano ai prodotti con elementi digitali contemplati dal presente regolamento.

(55) Conformemente al regolamento (UE) 2019/1020, le autorità di vigilanza del mercato effettuano la vigilanza del mercato nel territorio del rispettivo Stato membro. Il presente regolamento non dovrebbe impedire agli Stati membri di scegliere le autorità competenti incaricate dello svolgimento di tali compiti. Ogni Stato membro dovrebbe designare una o più autorità di vigilanza del mercato nel proprio territorio. Gli Stati membri possono scegliere di designare qualsiasi autorità già esistente o una nuova autorità che agisca come autorità di vigilanza del mercato, comprese le autorità nazionali competenti di cui all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)] o le autorità nazionali di certificazione della cibersicurezza designate di cui all'articolo 58 del regolamento (UE) 2019/881. Gli operatori economici dovrebbero collaborare pienamente con le autorità di vigilanza del mercato e con le altre autorità competenti. Ogni Stato membro dovrebbe informare la Commissione e gli altri Stati membri circa le sue autorità di vigilanza del mercato e gli ambiti di competenza di ciascuna autorità e garantire le risorse e le competenze necessarie per svolgere i compiti di vigilanza relativi al presente regolamento. A norma dell'articolo 10, paragrafi 2 e 3, del regolamento (UE) 2019/1020, ogni Stato membro dovrebbe designare un ufficio unico di collegamento responsabile, tra l'altro, di rappresentare la posizione coordinata delle autorità di vigilanza del mercato e di fornire sostegno alla cooperazione tra le autorità di vigilanza del mercato di diversi Stati membri.

(56) È opportuno istituire un apposito gruppo di cooperazione amministrativa (ADCO) per l'applicazione uniforme del presente regolamento, a norma dell'articolo 30, paragrafo 2, del regolamento (UE) 2019/1020. Tale ADCO dovrebbe essere composto da rappresentanti delle autorità di vigilanza del mercato designate e, se del caso, da rappresentanti degli uffici unici di collegamento. La Commissione dovrebbe sostenere e incoraggiare la cooperazione tra le autorità di vigilanza del mercato attraverso la rete dell'Unione per la conformità dei prodotti istituita sulla base dell'articolo 29 del

[20] Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011 (GU L 169 del 25.6.2019, pag. 1).

regolamento (UE) 2019/1020 e composta da rappresentanti di ciascuno Stato membro, inclusi un rappresentante degli uffici unici di collegamento di cui all'articolo 10 di tale regolamento, e un esperto nazionale opzionale, i presidenti degli ADCO e rappresentanti della Commissione. La Commissione dovrebbe partecipare alle riunioni della rete, dei suoi sottogruppi e di questo ADCO. Dovrebbe inoltre assistere quest'ultimo attraverso una segreteria esecutiva che fornisce supporto tecnico e logistico.

(57) Al fine di garantire misure tempestive, proporzionate ed efficaci in relazione ai prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo, è opportuno prevedere una procedura di salvaguardia dell'Unione in base alla quale le parti interessate siano informate delle misure che si intendono adottare per quanto riguarda tali prodotti. Ciò dovrebbe consentire inoltre alle autorità di vigilanza del mercato, in cooperazione con gli operatori economici interessati, di intervenire in una fase precoce, ove necessario. Nei casi in cui gli Stati membri e la Commissione concordino sul fatto che una misura presa da uno Stato membro sia giustificata, dovrebbero essere previsti ulteriori interventi da parte della Commissione, tranne qualora la non conformità possa essere attribuita a carenze di una norma armonizzata.

(58) In alcuni casi un prodotto con elementi digitali conforme al presente regolamento può tuttavia presentare un rischio di cibersicurezza significativo o comportare un rischio per la salute o la sicurezza delle persone, per la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali, per la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti utilizzando un sistema di informazione elettronico da parte di soggetti essenziali del tipo di cui [all'allegato I della direttiva XXX/XXXX (NIS2)] o per altri aspetti della tutela dell'interesse pubblico. È quindi necessario stabilire norme che garantiscano l'attenuazione di tali rischi. Di conseguenza le autorità di vigilanza del mercato dovrebbero adottare misure per imporre all'operatore economico di garantire che il prodotto non presenti più tale rischio oppure di richiamarlo o di ritirarlo, a seconda del rischio. Non appena un'autorità di vigilanza del mercato limita o vieta in tal modo la libera circolazione di un prodotto, lo Stato membro dovrebbe notificare senza indugio alla Commissione e agli altri Stati membri le misure provvisorie, indicando motivi e giustificazioni della decisione. Qualora un'autorità di vigilanza del mercato adotti tali misure contro prodotti che presentano un rischio, la Commissione dovrebbe avviare senza indugio consultazioni con gli Stati membri e con l'operatore o gli operatori economici interessati e valutare la misura nazionale. In base ai risultati di tale valutazione, la Commissione dovrebbe decidere se la misura nazionale sia giustificata o meno. La Commissione dovrebbe indirizzare la sua decisione a tutti gli Stati membri e comunicarla immediatamente ad essi e all'operatore o agli operatori economici interessati. Se la misura è ritenuta giustificata, la Commissione può anche prendere in considerazione l'adozione di proposte per rivedere la corrispondente normativa dell'Unione.

(59) Per i prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo e qualora vi sia motivo di ritenere che non siano conformi al presente regolamento o per i prodotti conformi al presente regolamento, ma che presentano altri rischi gravi, quali i rischi per la salute o la sicurezza delle persone, per i diritti fondamentali o per la fornitura dei servizi da parte dei soggetti essenziali del tipo di cui [all'allegato I della direttiva XXX/XXXX (NIS2)], la Commissione può chiedere all'ENISA di effettuare una valutazione. Sulla base di tale valutazione, la Commissione può adottare, mediante atti di esecuzione, misure correttive o restrittive

a livello dell'Unione, tra cui l'ordine di ritiro dal mercato o il richiamo dei prodotti in questione, entro un termine ragionevole, proporzionato alla natura del rischio. La Commissione può ricorrere a tale intervento solo in circostanze eccezionali che giustifichino un intervento immediato per preservare il buon funzionamento del mercato interno e solo nel caso in cui le autorità di vigilanza non abbiano adottato misure efficaci per porre rimedio alla situazione. Tali circostanze eccezionali possono essere situazioni di emergenza in cui, ad esempio, il fabbricante mette ampiamente a disposizione, in diversi Stati membri, un prodotto non conforme che è utilizzato anche in settori essenziali dai soggetti che rientrano nell'ambito di applicazione della [direttiva XXX/XXXX (NIS2)] e che contiene vulnerabilità note sfruttate da soggetti malintenzionati, per le quali il fabbricante non prevede la disponibilità di patch. La Commissione può intervenire in tali situazioni di emergenza solo per la durata delle circostanze eccezionali e se la non conformità al presente regolamento o i gravi rischi presentati persistono.

(60) Nei casi in cui vi siano indicazioni di non conformità al presente regolamento in diversi Stati membri, le autorità di vigilanza del mercato dovrebbero poter svolgere attività congiunte con altre autorità al fine di verificare la conformità e individuare i rischi di cibersicurezza dei prodotti con elementi digitali.

(61) Le azioni di controllo coordinate e simultanee ("indagini a tappeto"), che sono intraprese dalle autorità di vigilanza del mercato con l'obiettivo specifico di controllare l'osservanza delle norme, possono migliorare ulteriormente la sicurezza dei prodotti. In particolare dovrebbero essere condotte indagini a tappeto laddove le tendenze del mercato, i reclami dei consumatori o altri elementi indichino che talune categorie di prodotti spesso presentano rischi di cibersicurezza. L'ENISA dovrebbe presentare alle autorità di vigilanza del mercato proposte di categorie di prodotti per le quali potrebbero essere organizzate indagini a tappeto, basandosi, tra l'altro, sulle notifiche ricevute riguardanti le vulnerabilità e gli incidenti relativi ai prodotti.

(62) Al fine di garantire che il quadro normativo possa essere adattato ove necessario, alla Commissione dovrebbe essere delegato il potere di adottare atti conformemente all'articolo 290 TFUE per aggiornare l'elenco dei prodotti critici di cui all'allegato III e per specificare le definizioni di tali categorie di prodotti. Alla Commissione dovrebbe essere delegato il potere di adottare atti conformemente a tale articolo per individuare i prodotti con elementi digitali disciplinati da altre norme dell'Unione che conseguono lo stesso livello di protezione del presente regolamento, specificando se sia necessaria una limitazione o un'esclusione dall'ambito di applicazione del presente regolamento nonché la portata di tale limitazione, ove applicabile. Alla Commissione dovrebbe essere delegato il potere di adottare atti conformemente a tale articolo anche per quanto riguarda l'eventuale obbligo di certificazione di determinati prodotti con elementi digitali altamente critici sulla base dei criteri di criticità stabiliti nel presente regolamento, nonché per specificare il contenuto minimo della dichiarazione di conformità UE e integrare gli elementi da includere nella documentazione tecnica. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[21]. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli

[21] GU L 123 del 12.5.2016, pag. 1.

esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

(63) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire alla Commissione competenze di esecuzione per: specificare il formato e gli elementi della distinta base del software, specificare ulteriormente il tipo di informazioni, il formato e la procedura delle notifiche trasmesse all'ENISA dai fabbricanti riguardo alle vulnerabilità attivamente sfruttate e agli incidenti, specificare i sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che possono essere utilizzati per dimostrare la conformità ai requisiti essenziali o a parti di essi di cui all'allegato I del presente regolamento, adottare specifiche comuni per quanto riguarda i requisiti essenziali di cui all'allegato I, stabilire le specifiche tecniche per i pittogrammi o qualsiasi altro marchio relativo alla sicurezza dei prodotti con elementi digitali e i meccanismi per promuoverne l'uso, e decidere in merito a misure correttive o restrittive a livello dell'Unione in circostanze eccezionali che giustifichino un intervento immediato per preservare il buon funzionamento del mercato interno. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio[22].

(64) Al fine di garantire una cooperazione affidabile e costruttiva delle autorità di vigilanza del mercato a livello nazionale e dell'Unione, è opportuno che tutte le parti coinvolte nell'applicazione del presente regolamento rispettino la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti.

(65) Per garantire l'effettiva applicazione degli obblighi previsti dal presente regolamento, ogni autorità di vigilanza del mercato dovrebbe avere il potere di imporre o richiedere l'imposizione di sanzioni amministrative pecuniarie. È pertanto opportuno stabilire i livelli massimi delle sanzioni amministrative pecuniarie che devono essere previste negli ordinamenti nazionali in caso di mancato rispetto degli obblighi stabiliti dal presente regolamento. Nel decidere l'importo della sanzione amministrativa pecuniaria in ogni singolo caso si dovrebbe tenere conto di tutte le circostanze pertinenti della situazione specifica e, come minimo, di quelle esplicitamente stabilite nel presente regolamento, compresa l'eventualità che altre autorità di vigilanza del mercato abbiano già applicato sanzioni amministrative pecuniarie allo stesso operatore per violazioni analoghe. Tali circostanze possono costituire un'aggravante, nel caso in cui la violazione da parte dello stesso operatore si ripeta sul territorio di Stati membri diversi da quello in cui è già stata applicata una sanzione amministrativa pecuniaria, o un'attenuante, in quanto garantiscono che qualsiasi altra sanzione amministrativa pecuniaria presa in considerazione da un'altra autorità di vigilanza del mercato per lo stesso operatore economico o per lo stesso tipo di violazione tenga già conto, insieme ad altre circostanze specifiche pertinenti, di una sanzione e del suo importo imposti in altri Stati membri. In tutti questi casi la sanzione amministrativa pecuniaria cumulativa che le autorità di vigilanza del mercato di diversi Stati membri potrebbero applicare allo stesso operatore economico per lo stesso tipo di violazione dovrebbe garantire il rispetto del principio di proporzionalità.

---

[22] Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

(66) Se le sanzioni amministrative pecuniarie sono inflitte a persone che non sono imprese, l'autorità competente dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie.

(67) Nei suoi rapporti con i paesi terzi l'UE si sforza di promuovere il commercio internazionale di prodotti soggetti a regolamentazione. Per agevolare gli scambi è possibile applicare un'ampia gamma di misure, tra cui diversi strumenti giuridici come gli accordi sul reciproco riconoscimento (ARR) bilaterali (intergovernativi) in materia di valutazione della conformità e marcatura dei prodotti soggetti a regolamentazione. Gli ARR sono conclusi tra l'Unione e i paesi terzi che presentano un livello comparabile di sviluppo tecnico e un approccio compatibile riguardo alla valutazione della conformità. Questi accordi si basano sulla reciproca accettazione di certificati, marchi di conformità e rapporti di prova rilasciati dagli organismi di valutazione della conformità di una parte conformemente alla normativa dell'altra parte. Attualmente sono in vigore ARR per diversi paesi. Gli accordi sono conclusi in alcuni settori specifici, che possono variare da paese a paese. Al fine di agevolare ulteriormente gli scambi e riconoscendo che le catene di approvvigionamento dei prodotti con elementi digitali sono globali, l'Unione può concludere ARR relativi alla valutazione della conformità per i prodotti disciplinati dal presente regolamento, conformemente all'articolo 218 TFUE. Anche la cooperazione con i paesi partner è importante per aumentare la ciberresilienza a livello globale, poiché a lungo termine ciò contribuirà a rafforzare il quadro della cibersicurezza sia all'interno che all'esterno dell'UE.

(68) È opportuno che la Commissione riesamini il presente regolamento a scadenze regolari, in consultazione con le parti interessate, in particolare al fine di valutare la necessità di modifiche alla luce dei cambiamenti delle condizioni sociali, politiche, tecnologiche o del mercato.

(69) Agli operatori economici dovrebbe essere concesso un periodo di tempo sufficiente per adeguarsi ai requisiti del presente regolamento. Il presente regolamento dovrebbe applicarsi [24 mesi] dopo la sua entrata in vigore, ad eccezione degli obblighi di segnalazione delle vulnerabilità attivamente sfruttate e degli incidenti, che dovrebbero applicarsi [12 mesi] dopo l'entrata in vigore del presente regolamento.

(70) Poiché l'obiettivo del presente regolamento non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo degli effetti dell'azione in oggetto, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(71) Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[23] e ha espresso un parere il […],

---

[23] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto

Il presente regolamento stabilisce:

a) norme per l'immissione sul mercato di prodotti con elementi digitali per garantire la cibersicurezza di tali prodotti;

b) requisiti essenziali per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali e obblighi per gli operatori economici in relazione a tali prodotti per quanto riguarda la cibersicurezza;

c) requisiti essenziali per i processi di gestione delle vulnerabilità messi in atto dai fabbricanti per garantire la cibersicurezza dei prodotti con elementi digitali durante l'intero ciclo di vita e obblighi per gli operatori economici in relazione a tali processi;

d) norme sulla vigilanza del mercato e sull'applicazione delle norme e dei requisiti di cui sopra.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica ai prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete.

2. Il presente regolamento non si applica ai prodotti con elementi digitali a cui si applicano i seguenti atti dell'Unione:

   a) regolamento (UE) 2017/745;

   b) regolamento (UE) 2017/746;

   c) regolamento (UE) 2019/2144.

3. Il presente regolamento non si applica ai prodotti con elementi digitali che sono stati certificati in conformità del regolamento (UE) 2018/1139.

4. L'applicazione del presente regolamento ai prodotti con elementi digitali contemplati da altre norme dell'Unione, che stabiliscono requisiti che affrontano tutti o alcuni rischi coperti dai requisiti essenziali di cui all'allegato I, può essere limitata o esclusa, qualora:

   a) tale limitazione o esclusione sia coerente con il quadro normativo generale applicabile a tali prodotti; e

   b) le norme settoriali conseguano lo stesso livello di protezione previsto dal presente regolamento.

   Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 50 per modificare il presente regolamento specificando se tale limitazione

o esclusione sia necessaria, i prodotti e le norme interessati, nonché la portata della limitazione, se pertinente.

5. Il presente regolamento non si applica ai prodotti con elementi digitali sviluppati esclusivamente per scopi di sicurezza nazionale o militari o ai prodotti specificamente progettati per trattare informazioni classificate.

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) "prodotto con elementi digitali": qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware da immettere sul mercato separatamente;

2) "elaborazione dati da remoto": qualsiasi elaborazione dati a distanza per la quale il software è stato progettato e sviluppato dal fabbricante o sotto la sua responsabilità e la cui assenza impedirebbe al prodotto con elementi digitali di svolgere una delle sue funzioni;

3) "prodotto con elementi digitali critico": un prodotto con elementi digitali che presenta un rischio di cibersicurezza secondo i criteri di cui all'articolo 6, paragrafo 2, e la cui funzionalità principale è indicata nell'allegato III;

4) "prodotto con elementi digitali altamente critico": un prodotto con elementi digitali che presenta un rischio di cibersicurezza secondo i criteri di cui all'articolo 6, paragrafo 5;

5) "tecnologia operativa": sistemi o dispositivi digitali programmabili che interagiscono con l'ambiente fisico o che gestiscono dispositivi che interagiscono con l'ambiente fisico;

6) "software": la parte di un sistema di informazione elettronico costituita da un codice informatico;

7) "hardware": un sistema di informazione elettronico fisico, o parti di esso, in grado di trattare, conservare o trasmettere dati digitali;

8) "componente": il software o l'hardware destinato a essere integrato in un sistema di informazione elettronico;

9) "sistema di informazione elettronico": qualsiasi sistema, comprese le apparecchiature elettriche o elettroniche, in grado di trattare, conservare o trasmettere dati digitali;

10) "connessione logica": una rappresentazione virtuale di una connessione dati realizzata attraverso un'interfaccia software;

11) "connessione fisica": qualsiasi connessione tra sistemi di informazione elettronici o componenti realizzata con mezzi fisici, anche attraverso interfacce elettriche o meccaniche, fili od onde radio;

12) "connessione indiretta": una connessione a un dispositivo o a una rete che non avviene direttamente, ma piuttosto nell'ambito di un sistema più ampio che è direttamente collegabile a tale dispositivo o rete;

13) "privilegio": un diritto di accesso concesso a determinati utenti o programmi per eseguire operazioni rilevanti per la sicurezza all'interno di un sistema di informazione elettronico;

14) "privilegio elevato": un diritto di accesso concesso a particolari utenti o programmi per eseguire un'ampia serie di operazioni rilevanti per la sicurezza all'interno di un sistema di informazione elettronico che, se utilizzato in modo improprio o compromesso, potrebbe consentire a soggetti malintenzionati di ottenere un accesso più ampio alle risorse di un sistema o di un'organizzazione;

15) "endpoint": qualsiasi dispositivo connesso a una rete e che funge da punto di accesso a tale rete;

16) "risorse di rete o informatiche": dati o funzionalità hardware o software accessibili localmente o attraverso una rete o un altro dispositivo connesso;

17) "operatore economico": il fabbricante, il rappresentante autorizzato, l'importatore, il distributore o qualsiasi altra persona fisica o giuridica soggetta agli obblighi stabiliti dal presente regolamento;

18) "fabbricante": qualsiasi persona fisica o giuridica che sviluppi o fabbrichi prodotti con elementi digitali o che faccia progettare, sviluppare o fabbricare prodotti con elementi digitali e li commercializzi con il proprio nome o marchio, a titolo oneroso o gratuito;

19) "rappresentante autorizzato": qualsiasi persona fisica o giuridica stabilita nell'Unione che abbia ricevuto da un fabbricante un mandato scritto che la autorizza ad agire per suo conto in relazione a determinati compiti;

20) "importatore": qualsiasi persona fisica o giuridica stabilita nell'Unione che immette sul mercato un prodotto con elementi digitali recante il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione;

21) "distributore": qualsiasi persona fisica o giuridica nella catena di approvvigionamento, diversa dal fabbricante o dall'importatore, che mette a disposizione un prodotto con elementi digitali sul mercato dell'Unione senza modificarne le proprietà;

22) "immissione sul mercato": la prima messa a disposizione di un prodotto con elementi digitali sul mercato dell'Unione;

23) "messa a disposizione sul mercato": la fornitura, a titolo oneroso o gratuito, di un prodotto con elementi digitali perché sia distribuito o usato sul mercato dell'Unione nel corso di un'attività commerciale;

24) "finalità prevista": l'uso di un prodotto con elementi digitali previsto dal fabbricante, compresi il contesto e le condizioni d'uso specifici, come dettagliati nelle informazioni comunicate dal fabbricante nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica;

25) "uso ragionevolmente prevedibile": un uso che non corrisponde necessariamente alla finalità prevista dal fabbricante nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica, ma che è probabile possa derivare da un comportamento umano o da operazioni o interazioni tecniche ragionevolmente prevedibili;

26) "uso improprio ragionevolmente prevedibile": l'uso di un prodotto con elementi digitali in un modo non conforme alla sua finalità prevista, ma che può derivare da un comportamento umano o da un'interazione con altri sistemi ragionevolmente prevedibili;

27) "autorità di notifica": l'autorità nazionale responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio;

28) "valutazione della conformità": il processo atto a verificare il rispetto dei requisiti essenziali di cui all'allegato I;

29) "organismo di valutazione della conformità": l'organismo definito all'articolo 2, punto 13, del regolamento (UE) n. 765/2008;

30) "organismo notificato": un organismo di valutazione della conformità designato in conformità dell'articolo 33 del presente regolamento e di altre pertinenti normative di armonizzazione dell'Unione;

31) "modifica sostanziale": una modifica del prodotto con elementi digitali a seguito della sua immissione sul mercato che incide sulla conformità del prodotto con elementi digitali ai requisiti essenziali di cui all'allegato I, sezione 1, o comporta una modifica dell'uso previsto per il quale il prodotto con elementi digitali è stato valutato;

32) "marcatura CE": una marcatura mediante cui un fabbricante indica che un prodotto con elementi digitali e i processi messi in atto dal fabbricante sono conformi ai requisiti essenziali di cui all'allegato I e ad altre normative applicabili dell'Unione che armonizzano le condizioni per la commercializzazione dei prodotti ("normative di armonizzazione dell'Unione") e che ne prevedono l'apposizione;

33) "autorità di vigilanza del mercato": un'autorità quale definita all'articolo 3, punto 4, del regolamento (UE) 2019/1020;

34) "norma armonizzata": una norma armonizzata, quale definita all'articolo 2, punto 1, lettera c), del regolamento (UE) n. 1025/2012;

35) "rischio di cibersicurezza": il rischio definito all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)];

36) "rischio di cibersicurezza significativo": un rischio di cibersicurezza che, in base alle sue caratteristiche tecniche, si può presumere abbia una probabilità elevata di provocare un incidente che potrebbe avere un impatto negativo grave, causando anche notevoli perdite o perturbazioni materiali o non materiali;

37) "distinta base del software": un registro formale contenente i dettagli e le relazioni della catena di approvvigionamento dei componenti inclusi negli elementi software di un prodotto con elementi digitali;

38) "vulnerabilità": una vulnerabilità definita all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)];

39) "vulnerabilità attivamente sfruttata": una vulnerabilità per la quale esistono prove attendibili che un soggetto ha proceduto all'esecuzione di un codice maligno su un sistema senza l'autorizzazione del proprietario del sistema;

40) "dati personali": i dati quali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679.

Articolo 4

Libera circolazione

1. Gli Stati membri non impediscono, per gli aspetti disciplinati dal presente regolamento, la messa a disposizione sul mercato di prodotti con elementi digitali che sono conformi al presente regolamento.

2. In occasione di fiere, mostre e dimostrazioni o eventi analoghi, gli Stati membri non impediscono la presentazione e l'uso di un prodotto con elementi digitali non conforme al presente regolamento.

3. Gli Stati membri non impediscono la messa a disposizione di un software non finito non conforme al presente regolamento, a condizione che il software sia reso disponibile solo per un periodo limitato necessario ai fini di prova e che un'indicazione visibile specifichi chiaramente che non è conforme al presente regolamento e non sarà disponibile sul mercato per fini diversi dalla prova.

Articolo 5

Requisiti per i prodotti con elementi digitali

I prodotti con elementi digitali sono messi a disposizione sul mercato soltanto se:

1) soddisfano i requisiti essenziali di cui all'allegato I, sezione 1, a condizione che siano correttamente installati, siano oggetto di un'adeguata manutenzione e siano utilizzati conformemente alla loro finalità prevista o in condizioni ragionevolmente prevedibili e, se opportuno, aggiornati, e

2) i processi messi in atto dal fabbricante sono conformi ai requisiti essenziali di cui all'allegato I, sezione 2.

Articolo 6

Prodotti con elementi digitali critici

1. I prodotti con elementi digitali che appartengono a una categoria di cui all'allegato III sono considerati prodotti con elementi digitali critici. I prodotti che hanno la funzionalità principale di una categoria di cui all'allegato III del presente regolamento sono considerati come appartenenti a tale categoria. Le categorie di prodotti con elementi digitali critici sono suddivise nella classe I e nella classe II, come indicato nell'allegato III, che riflettono il livello di rischio di cibersicurezza relativo a tali prodotti.

2. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 50 al fine di modificare l'allegato III, includendo nell'elenco delle categorie di prodotti con elementi digitali critici una nuova categoria o eliminandone una esistente. Nel valutare la necessità di modificare l'elenco di cui all'allegato III, la Commissione tiene conto del livello di rischio di cibersicurezza relativo alla categoria di prodotti con elementi digitali. Per la determinazione del livello di rischio di cibersicurezza si tiene conto di uno o più dei criteri indicati di seguito:

   a) la funzionalità legata alla cibersicurezza del prodotto con elementi digitali e se il prodotto con elementi digitali ha almeno uno degli attributi seguenti:

      i) è progettato per funzionare con privilegi elevati o per gestire privilegi;

      ii) ha accesso diretto o privilegiato alle risorse di rete o informatiche;

iii) è progettato per controllare l'accesso ai dati o alla tecnologia operativa;

iv) svolge una funzione critica per la fiducia, in particolare funzioni di sicurezza come il controllo della rete, la sicurezza degli endpoint e la protezione della rete;

b) l'uso previsto in ambienti sensibili, compresi quelli industriali o da parte di soggetti essenziali del tipo di cui all'allegato [allegato I] della direttiva [direttiva XXX/XXXX (NIS2)];

c) l'uso previsto per lo svolgimento di funzioni critiche o sensibili, come il trattamento dei dati personali;

d) la portata potenziale di un impatto negativo, in particolare in termini di intensità e capacità di incidere su una pluralità di persone;

e) la misura in cui l'uso di prodotti con elementi digitali ha già causato perdite o perturbazioni materiali o non materiali o ha suscitato preoccupazioni significative in relazione al verificarsi di un impatto negativo.

3. Alla Commissione è conferito il potere di adottare un atto delegato conformemente all'articolo 50 per integrare il presente regolamento, specificando le definizioni delle categorie di prodotti delle classi I e II di cui all'allegato III. L'atto delegato è adottato [entro 12 mesi dall'entrata in vigore del presente regolamento].

4. I prodotti con elementi digitali critici sono soggetti alle procedure di valutazione della conformità di cui all'articolo 24, paragrafi 2 e 3.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 50 per integrare il presente regolamento, specificando le categorie di prodotti con elementi digitali altamente critici per i quali i fabbricanti sono tenuti a ottenere un certificato europeo di cibersicurezza nell'ambito di un sistema europeo di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881 per dimostrare la conformità ai requisiti essenziali di cui all'allegato I o a loro parti. Nel determinare tali categorie di prodotti con elementi digitali altamente critici, la Commissione tiene conto del livello di rischio di cibersicurezza relativo alla categoria di prodotti con elementi digitali, alla luce di uno o più dei criteri di cui al paragrafo 2, nonché in considerazione della valutazione se tale categoria di prodotti:

a) sia utilizzata dai soggetti essenziali del tipo di cui all'allegato [allegato I] della direttiva [direttiva XXX/XXXX (NIS2)], sia una categoria di prodotti su cui detti soggetti fanno affidamento, oppure possa avere un'importanza futura per le attività di tali soggetti; o

b) sia pertinente per la resilienza dell'intera catena di approvvigionamento dei prodotti con elementi digitali contro eventi perturbatori.

Articolo 7

Sicurezza generale dei prodotti

In deroga all'articolo 2, paragrafo 1, terzo comma, lettera b), del regolamento [regolamento relativo alla sicurezza generale dei prodotti], qualora i prodotti con elementi digitali non siano soggetti a requisiti specifici imposti da altre normative di armonizzazione dell'Unione ai sensi dell'[articolo 3, punto 25, del regolamento sulla sicurezza generale dei prodotti], il capo III, sezione 1, i capi V e VII e i capi da IX a XI del regolamento [regolamento relativo alla

sicurezza generale dei prodotti] si applicano a tali prodotti per quanto riguarda i rischi di sicurezza non contemplati dal presente regolamento.

Articolo 8

Sistemi di IA ad alto rischio

1. I prodotti con elementi digitali classificati come sistemi di IA ad alto rischio conformemente all'articolo [articolo 6] del regolamento [regolamento sull'IA] che rientrano nell'ambito di applicazione del presente regolamento e che soddisfano i requisiti essenziali di cui all'allegato I, sezione 1, del presente regolamento, laddove i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cui all'allegato I, sezione 2, sono considerati conformi ai requisiti relativi alla cibersicurezza di cui all'articolo [articolo 15] del regolamento [regolamento sull'IA], fatti salvi gli altri requisiti relativi all'accuratezza e alla robustezza inclusi nel suddetto articolo e nella misura in cui il conseguimento del livello di protezione previsto da tali requisiti sia dimostrato dalla dichiarazione di conformità UE rilasciata a norma del presente regolamento.

2. Per quanto riguarda i prodotti e i requisiti di cibersicurezza di cui al paragrafo 1, si applica la pertinente procedura di valutazione della conformità prevista dall'articolo [articolo 43] del regolamento [regolamento sull'IA]. Ai fini di tale valutazione, gli organismi notificati che sono autorizzati a controllare la conformità dei sistemi di IA ad alto rischio a norma del regolamento [regolamento sull'IA] sono anche autorizzati a controllare la conformità dei sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del presente regolamento ai requisiti di cui all'allegato I del presente regolamento, a condizione che la conformità di tali organismi notificati ai requisiti di cui all'articolo 29 del presente regolamento sia stata valutata nel contesto della procedura di notifica di cui al regolamento [regolamento sull'IA].

3. In deroga al paragrafo 2, i prodotti con elementi digitali critici di cui all'allegato III del presente regolamento che devono applicare le procedure di valutazione della conformità di cui all'articolo 24, paragrafo 2, lettere a) e b), e paragrafo 3, lettere a) e b), a norma del presente regolamento, che sono anche classificati come sistemi di IA ad alto rischio conformemente all'articolo [articolo 6] del regolamento [regolamento sull'IA] e ai quali si applica la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato [allegato VI] del regolamento [regolamento sull'IA], sono soggetti alle procedure di valutazione della conformità previste dal presente regolamento per quanto riguarda i requisiti essenziali del presente regolamento.

Articolo 9

Prodotti macchina

I prodotti macchina che rientrano nell'ambito di applicazione del regolamento [proposta di regolamento sui prodotti macchina], che sono prodotti con elementi digitali ai sensi del presente regolamento e per i quali è stata rilasciata una dichiarazione di conformità UE sulla base di quest'ultimo si presumono conformi ai requisiti essenziali di sicurezza e di tutela della salute di cui all'allegato [allegato III, sezioni 1.1.9 e 1.2.1] del regolamento [proposta di regolamento sui prodotti macchina], per quanto concerne la protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo e nella misura in cui il conseguimento del

livello di protezione previsto da tali requisiti sia dimostrato nella dichiarazione di conformità UE rilasciata a norma del presente regolamento.

CAPO II

OBBLIGHI DEGLI OPERATORI ECONOMICI

Articolo 10

Obblighi dei fabbricanti

1. All'atto dell'immissione sul mercato di un prodotto con elementi digitali, i fabbricanti assicurano che sia stato progettato, sviluppato e prodotto conformemente ai requisiti essenziali di cui all'allegato I, sezione 1.

2. Ai fini dell'adempimento dell'obbligo di cui al paragrafo 1, i fabbricanti effettuano una valutazione dei rischi di cibersicurezza associati a un prodotto con elementi digitali e tengono conto dei risultati di tale valutazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto con elementi digitali, allo scopo di ridurre al minimo i rischi di cibersicurezza, prevenire gli incidenti di sicurezza e ridurre al minimo l'impatto di tali incidenti, anche in relazione alla salute e alla sicurezza degli utilizzatori.

3. All'atto dell'immissione sul mercato di un prodotto con elementi digitali, il fabbricante include una valutazione dei rischi di cibersicurezza nella documentazione tecnica di cui all'articolo 23 e all'allegato V. Per i prodotti con elementi digitali di cui all'articolo 8 e all'articolo 24, paragrafo 4, che sono soggetti anche ad altri atti dell'Unione, la valutazione dei rischi di cibersicurezza può far parte della valutazione dei rischi prevista da tali rispettivi atti dell'Unione. Se alcuni requisiti essenziali non sono applicabili al prodotto con elementi digitali commercializzato, il fabbricante fornisce una chiara giustificazione in tale documentazione.

4. Ai fini dell'adempimento dell'obbligo di cui al paragrafo 1, i fabbricanti esercitano la dovuta diligenza quando integrano componenti provenienti da terzi in prodotti con elementi digitali. Essi garantiscono che tali componenti non compromettano la sicurezza del prodotto con elementi digitali.

5. Il fabbricante documenta sistematicamente, in modo proporzionato alla natura e ai rischi di cibersicurezza, gli aspetti pertinenti di cibersicurezza relativi al prodotto con elementi digitali, comprese le vulnerabilità di cui viene a conoscenza e qualsiasi informazione pertinente fornita da terzi e, se del caso, aggiorna la valutazione dei rischi del prodotto.

6. All'atto dell'immissione sul mercato di un prodotto con elementi digitali e per la durata prevista del prodotto o per un periodo di cinque anni dall'immissione sul mercato del prodotto, a seconda di quale sia il periodo più breve, i fabbricanti garantiscono che le vulnerabilità di tale prodotto siano gestite in modo efficace e in conformità dei requisiti essenziali di cui all'allegato I, sezione 2.

   I fabbricanti dispongono di politiche e procedure adeguate, comprese politiche di divulgazione coordinata delle vulnerabilità, di cui all'allegato I, sezione 2, punto 5, per trattare e correggere potenziali vulnerabilità del prodotto con elementi digitali segnalate da fonti interne o esterne.

7. Prima di immettere un prodotto con elementi digitali sul mercato, i fabbricanti redigono la documentazione tecnica di cui all'articolo 23.

   Essi seguono o fanno eseguire le procedure di valutazione della conformità prescelte di cui all'articolo 24.

   Se tale procedura di valutazione della conformità dimostra la conformità del prodotto con elementi digitali ai requisiti essenziali di cui all'allegato I, sezione 1, e dei processi messi in atto dal fabbricante ai requisiti essenziali di cui all'allegato I, sezione 2, i fabbricanti redigono la dichiarazione di conformità UE conformemente all'articolo 20 e appongono la marcatura CE conformemente all'articolo 22.

8. I fabbricanti tengono la documentazione tecnica e la dichiarazione di conformità UE, se pertinente, a disposizione delle autorità di vigilanza del mercato per un periodo di dieci anni dalla data di immissione sul mercato del prodotto con elementi digitali.

9. I fabbricanti si assicurano che siano predisposte le procedure necessarie affinché i prodotti con elementi digitali fabbricati nell'ambito di una produzione in serie rimangano conformi. Il fabbricante tiene adeguatamente conto delle modifiche del processo di sviluppo e di produzione o della progettazione o delle caratteristiche del prodotto con elementi digitali, nonché delle modifiche delle norme armonizzate, dei sistemi europei di certificazione della cibersicurezza o delle specifiche comuni di cui all'articolo 19 con riferimento alle quali è dichiarata la conformità del prodotto con elementi digitali o mediante applicazione delle quali tale conformità è verificata.

10. I fabbricanti provvedono affinché i prodotti con elementi digitali siano accompagnati dalle informazioni e dalle istruzioni di cui all'allegato II in forma elettronica o fisica. Tali informazioni e istruzioni sono redatte in una lingua che possa essere facilmente compresa dagli utilizzatori. Sono chiare, comprensibili, intelligibili e leggibili. Consentono un'installazione, un funzionamento e un utilizzo sicuri dei prodotti con elementi digitali.

11. I fabbricanti forniscono la dichiarazione di conformità UE con il prodotto con elementi digitali o includono nelle istruzioni e nelle informazioni di cui all'allegato II l'indirizzo internet dove è possibile accedere alla dichiarazione di conformità UE.

12. A partire dall'immissione sul mercato e per la durata prevista del prodotto o per un periodo di cinque anni dall'immissione sul mercato di un prodotto con elementi digitali, a seconda di quale sia il periodo più breve, i fabbricanti che hanno la certezza o motivo di credere che il prodotto con elementi digitali o i processi messi in atto dal fabbricante non siano conformi ai requisiti essenziali di cui all'allegato I adottano immediatamente le misure correttive necessarie per rendere conformi il prodotto con elementi digitali o i processi del fabbricante oppure, a seconda dei casi, per ritirare o richiamare il prodotto.

13. I fabbricanti, a seguito di una richiesta motivata di un'autorità di vigilanza del mercato, forniscono a tale autorità, in una lingua che può essere facilmente compresa da quest'ultima, tutte le informazioni e la documentazione, in formato cartaceo o elettronico, necessarie a dimostrare la conformità del prodotto con elementi digitali e dei processi messi in atto dal fabbricante ai requisiti essenziali di cui all'allegato I. Essi cooperano con tale autorità, su richiesta di quest'ultima, in merito a qualsiasi misura adottata per eliminare i rischi di cibersicurezza presentati dal prodotto con elementi digitali che hanno immesso sul mercato.

14. Il fabbricante che cessa l'attività e di conseguenza non è in grado di adempiere agli obblighi previsti dal presente regolamento informa, prima che la cessazione

dell'attività abbia effetto, le autorità di vigilanza del mercato competenti di tale situazione, nonché, con ogni mezzo disponibile e nella misura del possibile, gli utilizzatori dei prodotti con elementi digitali interessati immessi sul mercato.

15. La Commissione può, mediante atti di esecuzione, specificare il formato e gli elementi della distinta base del software di cui all'allegato I, sezione 2, punto 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 51, paragrafo 2.

Articolo 11

Obblighi di segnalazione dei fabbricanti

1. Il fabbricante notifica all'ENISA, senza indebito ritardo e comunque entro 24 ore dal momento in cui ne è venuto a conoscenza, qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali. La notifica include i dettagli relativi a tale vulnerabilità e, se del caso, le misure correttive o di attenuazione adottate. Al momento di ricevimento della notifica, l'ENISA la trasmette senza indebito ritardo, a meno che non vi siano giustificati motivi legati al rischio di cibersicurezza, ai CSIRT degli Stati membri interessati designati ai fini della divulgazione coordinata delle vulnerabilità conformemente all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)] e informa l'autorità di vigilanza del mercato in merito alla vulnerabilità notificata.

2. Il fabbricante notifica all'ENISA, senza indebito ritardo e comunque entro 24 ore dal momento in cui ne è venuto a conoscenza, qualsiasi incidente che abbia un impatto sulla sicurezza del prodotto con elementi digitali. L'ENISA trasmette senza indebito ritardo, a meno che non vi siano giustificati motivi legati al rischio di cibersicurezza, le notifiche ai punti di contatto unici degli Stati membri interessati designati conformemente all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)] e informa l'autorità di vigilanza del mercato degli incidenti notificati. La notifica dell'incidente comprende informazioni sulla gravità e sull'impatto dell'incidente e, se del caso, indica se il fabbricante sospetta che l'incidente sia il risultato di atti illegittimi o malevoli o se ritiene che abbia un impatto transfrontaliero.

3. L'ENISA trasmette alla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), istituita dall'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)], le informazioni notificate a norma dei paragrafi 1 e 2, se tali informazioni sono pertinenti per la gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala a livello operativo.

4. Il fabbricante informa, senza indebito ritardo e dal momento in cui ne è venuto a conoscenza, gli utilizzatori del prodotto con elementi digitali in merito all'incidente e, se necessario, alle misure correttive che essi possono adottare per attenuarne l'impatto.

5. La Commissione può, mediante atti di esecuzione, specificare ulteriormente il tipo di informazioni, il formato e la procedura di trasmissione delle notifiche a norma dei paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 51, paragrafo 2.

6. L'ENISA prepara, sulla base delle notifiche ricevute a norma dei paragrafi 1 e 2, una relazione tecnica biennale sulle tendenze emergenti in materia di rischi di cibersicurezza nei prodotti con elementi digitali e la presenta al gruppo di

cooperazione di cui all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)]. La prima relazione di questo tipo è presentata entro 24 mesi dall'inizio dell'applicazione degli obblighi di cui ai paragrafi 1 e 2.

7. Quando è individuata una vulnerabilità in un componente, compreso un componente open source, integrato nel prodotto con elementi digitali, i fabbricanti la segnalano alla persona o al soggetto che si occupa della manutenzione di tale componente.

Articolo 12

Rappresentanti autorizzati

1. Un fabbricante può nominare un rappresentante autorizzato mediante un mandato scritto.

2. Gli obblighi di cui all'articolo 10, paragrafi da 1 a 7, primo comma, e paragrafo 9, non rientrano nel mandato del rappresentante autorizzato.

3. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fabbricante. Tale mandato consente al rappresentante autorizzato di svolgere almeno i seguenti compiti:

   a) mantenere a disposizione delle autorità di vigilanza del mercato la dichiarazione di conformità UE di cui all'articolo 20 e la documentazione tecnica di cui all'articolo 23 per un periodo di dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato;

   b) a seguito di una richiesta motivata di un'autorità di vigilanza del mercato, fornire a tale autorità tutte le informazioni e la documentazione necessarie a dimostrare la conformità del prodotto con elementi digitali;

   c) collaborare con le autorità di vigilanza del mercato, su richiesta di queste ultime, a qualsiasi azione intrapresa per eliminare i rischi presentati da un prodotto con elementi digitali che rientra nel suo mandato.

Articolo 13

Obblighi degli importatori

1. Gli importatori immettono sul mercato solo prodotti con elementi digitali conformi ai requisiti essenziali di cui all'allegato I, sezione 1, e laddove i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cui all'allegato I, sezione 2.

2. Prima di immettere un prodotto con elementi digitali sul mercato gli importatori si accertano che:

   a) il fabbricante abbia eseguito le procedure di valutazione della conformità appropriate di cui all'articolo 24;

   b) il fabbricante abbia redatto la documentazione tecnica;

   c) il prodotto con elementi digitali rechi la marcatura CE di cui all'articolo 22 e sia accompagnato dalle informazioni e dalle istruzioni per l'uso di cui all'allegato II.

3. Qualora ritenga o abbia motivo di credere che un prodotto con elementi digitali o i processi messi in atto dal fabbricante non siano conformi ai requisiti essenziali di cui all'allegato I, l'importatore non immette il prodotto sul mercato fino a quando il

prodotto o i processi messi in atto dal fabbricante non siano stati resi conformi ai requisiti essenziali di cui all'allegato I. Inoltre, se il prodotto con elementi digitali presenta un rischio di cibersicurezza significativo, l'importatore ne informa il fabbricante e le autorità di vigilanza del mercato.

4. Gli importatori indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato, l'indirizzo postale e l'indirizzo di posta elettronica ai quali possono essere contattati sul prodotto con elementi digitali oppure, ove ciò non sia possibile, sull'imballaggio o in un documento di accompagnamento del prodotto con elementi digitali. I dati di recapito sono redatti in una lingua facilmente comprensibile dagli utilizzatori e dalle autorità di vigilanza del mercato.

5. Gli importatori garantiscono che il prodotto con elementi digitali sia accompagnato dalle istruzioni e dalle informazioni di cui all'allegato II, redatte in una lingua facilmente comprensibile per gli utilizzatori.

6. Gli importatori che hanno la certezza o hanno motivo di credere che un prodotto con elementi digitali che hanno immesso sul mercato o i processi messi in atto dal suo fabbricante non siano conformi ai requisiti essenziali di cui all'allegato I adottano immediatamente le misure correttive necessarie per rendere tale prodotto con elementi digitali o i processi messi in atto dal suo fabbricante conformi ai requisiti essenziali di cui all'allegato I oppure, se del caso, per ritirare o richiamare il prodotto.

   Quando è individuata una vulnerabilità nel prodotto con elementi digitali, gli importatori ne informano il fabbricante senza indebito ritardo. Inoltre, se il prodotto con elementi digitali presenta un rischio di cibersicurezza significativo, gli importatori ne informano immediatamente le autorità di vigilanza del mercato degli Stati membri in cui hanno messo a disposizione sul mercato il prodotto con elementi digitali, dando in particolare informazioni dettagliate sulla non conformità e su eventuali misure correttive adottate.

7. Gli importatori mantengono una copia della dichiarazione di conformità UE a disposizione delle autorità di vigilanza del mercato per un periodo di dieci anni dalla data di immissione sul mercato del prodotto con elementi digitali e si accertano che la documentazione tecnica possa essere messa a disposizione di tali autorità, su richiesta.

8. A seguito di una richiesta motivata di un'autorità di vigilanza del mercato, gli importatori forniscono a quest'ultima, in formato cartaceo o elettronico, tutte le informazioni e la documentazione necessarie a dimostrare la conformità del prodotto con elementi digitali ai requisiti essenziali di cui all'allegato I, sezione 1, nonché la conformità dei processi messi in atto dal fabbricante ai requisiti essenziali di cui all'allegato I, sezione 2, in una lingua che possa essere facilmente compresa da tale autorità. Essi cooperano con tale autorità, su sua richiesta, a qualsiasi misura adottata per eliminare i rischi di cibersicurezza presentati da un prodotto con elementi digitali da essi immesso sul mercato.

9. Quando viene a conoscenza del fatto che il fabbricante di un prodotto con elementi digitali ha cessato l'attività e di conseguenza non è in grado di rispettare gli obblighi previsti dal presente regolamento, l'importatore di tale prodotto ne informa le autorità di vigilanza del mercato competenti nonché, con qualsiasi mezzo disponibile e nella misura del possibile, gli utilizzatori dei prodotti con elementi digitali immessi sul mercato.

Articolo 14

Obblighi dei distributori

1. Quando mettono un prodotto con elementi digitali a disposizione sul mercato, i distributori esercitano la dovuta diligenza per rispettare i requisiti del presente regolamento.

2. Prima di mettere un prodotto con elementi digitali a disposizione sul mercato, i distributori verificano che:

   a) il prodotto con elementi digitali rechi la marcatura CE;

   b) il fabbricante e l'importatore abbiano rispettato gli obblighi previsti rispettivamente dall'articolo 10, paragrafi 10 e 11, e dall'articolo 13, paragrafo 4.

3. Se un distributore ritiene o ha motivo di credere che un prodotto con elementi digitali o i processi messi in atto dal fabbricante non siano conformi ai requisiti essenziali di cui all'allegato I, il distributore non mette il prodotto con elementi digitali a disposizione sul mercato fino a quando il prodotto o i processi messi in atto dal fabbricante non siano stati resi conformi. Inoltre, quando il prodotto con elementi digitali presenta un rischio di cibersicurezza significativo, il distributore ne informa il fabbricante e le autorità di vigilanza del mercato.

4. I distributori che hanno la certezza o hanno motivo di credere che un prodotto con elementi digitali che hanno messo a disposizione sul mercato o i processi messi in atto dal suo fabbricante non siano conformi ai requisiti essenziali di cui all'allegato I si assicurano che siano adottate le misure correttive necessarie per rendere conformi tale prodotto con elementi digitali o i processi messi in atto dal suo fabbricante oppure, se del caso, per ritirare o richiamare il prodotto.

   Quando è individuata una vulnerabilità nel prodotto con elementi digitali, i distributori ne informano il fabbricante senza indebito ritardo. Inoltre, se il prodotto con elementi digitali presenta un rischio di cibersicurezza significativo, i distributori ne informano immediatamente le autorità di vigilanza del mercato degli Stati membri in cui hanno messo a disposizione sul mercato il prodotto con elementi digitali, dando in particolare informazioni dettagliate sulla non conformità e su eventuali misure correttive adottate.

5. A seguito di una richiesta motivata di un'autorità di vigilanza del mercato, i distributori forniscono a quest'ultima, in formato cartaceo o elettronico, tutte le informazioni e la documentazione necessarie a dimostrare la conformità del prodotto con elementi digitali e dei processi messi in atto dal suo fabbricante ai requisiti essenziali di cui all'allegato I in una lingua che possa essere facilmente compresa da tale autorità. Essi cooperano con tale autorità, su sua richiesta, a qualsiasi misura adottata per eliminare i rischi di cibersicurezza presentati da un prodotto con elementi digitali da essi messo a disposizione sul mercato.

6. Quando viene a conoscenza del fatto che il fabbricante di un prodotto con elementi digitali ha cessato l'attività e di conseguenza non è in grado di rispettare gli obblighi previsti dal presente regolamento, il distributore di tale prodotto ne informa le autorità di vigilanza del mercato competenti nonché, con qualsiasi mezzo disponibile e nella misura del possibile, gli utilizzatori dei prodotti con elementi digitali immessi sul mercato.

Articolo 15

Casi in cui gli obblighi dei fabbricanti si applicano agli importatori e ai distributori

Un importatore o distributore è ritenuto un fabbricante ai fini del presente regolamento, ed è soggetto agli obblighi del fabbricante di cui all'articolo 10 e all'articolo 11, paragrafi 1, 2, 4 e 7, quando immette sul mercato un prodotto con elementi digitali con il proprio nome o marchio commerciale o apporta una modifica sostanziale a un prodotto con elementi digitali già immesso sul mercato.

Articolo 16

Altri casi in cui si applicano gli obblighi dei fabbricanti

Una persona fisica o giuridica, diversa dal fabbricante, dall'importatore o dal distributore, che apporta una modifica sostanziale al prodotto con elementi digitali è considerata un fabbricante ai fini del presente regolamento.

Tale persona è soggetta agli obblighi del fabbricante di cui all'articolo 10 e all'articolo 11, paragrafi 1, 2, 4 e 7, per la parte del prodotto interessata da tale modifica sostanziale oppure, se la modifica sostanziale incide sulla cibersicurezza del prodotto con elementi digitali nel suo complesso, per l'intero prodotto.

Articolo 17

Identificazione degli operatori economici

1. Gli operatori economici forniscono alle autorità di vigilanza del mercato, su richiesta e se le informazioni sono disponibili, le informazioni seguenti:

   a) nome e indirizzo di qualsiasi operatore economico che abbia fornito loro un prodotto con elementi digitali;

   b) nome e indirizzo di qualsiasi operatore economico cui essi abbiano fornito un prodotto con elementi digitali.

2. Gli operatori economici si assicurano di essere in grado di presentare le informazioni di cui al paragrafo 1 per dieci anni dal momento in cui sia stato loro fornito un prodotto con elementi digitali e per dieci anni dal momento in cui essi abbiano fornito il prodotto con elementi digitali.

CAPO III

CONFORMITÀ DEL PRODOTTO CON ELEMENTI DIGITALI

Articolo 18

Presunzione di conformità

1. I prodotti con elementi digitali e i processi messi in atto dal fabbricante che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* si presumono conformi ai requisiti essenziali oggetto di tali norme o parti di esse di cui all'allegato I.

2. I prodotti con elementi digitali e i processi messi in atto dal fabbricante che sono conformi alle specifiche comuni di cui all'articolo 19 si presumono conformi ai

requisiti essenziali di cui all'allegato I, nella misura in cui tali requisiti siano contemplati da tali specifiche comuni.

3. I prodotti con elementi digitali e i processi messi in atto dal fabbricante per i quali sono stati rilasciati un certificato o una dichiarazione di conformità UE nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma del regolamento (UE) 2019/881 e specificato al paragrafo 4 si presumono conformi ai requisiti essenziali di cui all'allegato I, nella misura in cui tali requisiti siano contemplati dal certificato di cibersicurezza o dalla dichiarazione di conformità UE o da loro parti.

4. Alla Commissione è conferito il potere di specificare, mediante atti di esecuzione, i sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 che possono essere utilizzati per dimostrare la conformità ai requisiti essenziali o a parti di essi di cui all'allegato I. Inoltre la Commissione specifica, ove applicabile, se un certificato di cibersicurezza rilasciato nell'ambito di tali sistemi sopprime l'obbligo per un fabbricante di effettuare una valutazione della conformità da parte di terzi per i requisiti corrispondenti, come previsto dall'articolo 24, paragrafo 2, lettere a) e b), e paragrafo 3, lettere a) e b). Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 51, paragrafo 2.

Articolo 19

Specifiche comuni

Se non esistono norme armonizzate di cui all'articolo 18, se la Commissione ritiene che le norme armonizzate pertinenti non siano sufficienti a soddisfare i requisiti del presente regolamento o a soddisfare la richiesta di normazione della Commissione, se vi sono ritardi ingiustificati nella procedura di normazione o se la richiesta di norme armonizzate da parte della Commissione non è stata accettata dalle organizzazioni europee di normazione, alla Commissione è conferito il potere di adottare, mediante atti di esecuzione, specifiche comuni per quanto riguarda i requisiti essenziali di cui all'allegato I. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 51, paragrafo 2.

Articolo 20

Dichiarazione di conformità UE

1. La dichiarazione di conformità UE è redatta dai fabbricanti in conformità dell'articolo 10, paragrafo 7, e attesta il rispetto dei requisiti essenziali applicabili di cui all'allegato I.

2. La dichiarazione di conformità UE ha la struttura tipo di cui all'allegato IV e contiene gli elementi specificati nelle pertinenti procedure di valutazione della conformità di cui all'allegato VI. Tale dichiarazione è continuamente aggiornata. È resa disponibile nella lingua o nelle lingue richieste dallo Stato membro sul cui mercato il prodotto con elementi digitali è immesso o messo a disposizione.

3. Se al prodotto con elementi digitali si applicano più atti dell'Unione che prescrivono una dichiarazione di conformità UE, è redatta un'unica dichiarazione di conformità UE in rapporto a tutti questi atti dell'Unione. La dichiarazione contiene gli estremi degli atti dell'Unione in questione, compresi i riferimenti della loro pubblicazione.

4. Con la dichiarazione di conformità UE il fabbricante si assume la responsabilità della conformità del prodotto.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 50 per integrare il presente regolamento aggiungendo elementi al contenuto minimo della dichiarazione di conformità UE di cui all'allegato IV per tenere conto degli sviluppi tecnologici.

Articolo 21

Principi generali della marcatura CE

La marcatura CE di cui all'articolo 3, punto 32, è soggetta ai principi generali stabiliti all'articolo 30 del regolamento (CE) n. 765/2008.

Articolo 22

Regole e condizioni per l'apposizione della marcatura CE

1. La marcatura CE è apposta sul prodotto con elementi digitali in modo visibile, leggibile e indelebile. Qualora ciò non sia possibile o la natura del prodotto con elementi digitali non lo consenta, essa è apposta sull'imballaggio e sulla dichiarazione di conformità UE di cui all'articolo 20 che accompagna il prodotto con elementi digitali. Per i prodotti con elementi digitali sotto forma di software, la marcatura CE è apposta sulla dichiarazione di conformità UE di cui all'articolo 20 o sul sito web che accompagna il prodotto software.

2. A seconda della natura del prodotto con elementi digitali, l'altezza della marcatura CE apposta su di esso può essere inferiore a 5 mm, purché rimanga visibile e leggibile.

3. La marcatura CE è apposta sul prodotto con elementi digitali prima della sua immissione sul mercato. Può essere seguita da un pittogramma o da qualsiasi altro marchio che indichi un rischio o un impiego particolare stabilito negli atti di esecuzione di cui al paragrafo 6.

4. La marcatura CE è seguita dal numero di identificazione dell'organismo notificato, qualora quest'ultimo partecipi alla procedura di valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'articolo 24.

   Il numero di identificazione dell'organismo notificato è apposto dall'organismo stesso o, in base alle istruzioni di quest'ultimo, dal fabbricante o dal rappresentante autorizzato del fabbricante.

5. Gli Stati membri si avvalgono dei meccanismi esistenti per garantire un'applicazione corretta del regime che disciplina la marcatura CE e promuovono le azioni opportune contro l'uso improprio di tale marcatura. Qualora il prodotto con elementi digitali sia soggetto ad altri atti legislativi dell'Unione che prevedono l'apposizione della marcatura CE, questa indica che il prodotto rispetta anche i requisiti di tali altri atti legislativi.

6. La Commissione può, mediante atti di esecuzione, stabilire specifiche tecniche per i pittogrammi o qualsiasi altro marchio relativo alla sicurezza dei prodotti con elementi digitali e meccanismi per promuoverne l'uso. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 51, paragrafo 2.

Articolo 23

Documentazione tecnica

1. La documentazione tecnica contiene tutti i dati o i dettagli pertinenti relativi ai mezzi utilizzati dal fabbricante per garantire che il prodotto con elementi digitali e i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cui all'allegato I. Essa contiene almeno gli elementi di cui all'allegato V.

2. La documentazione tecnica è redatta prima dell'immissione sul mercato del prodotto con elementi digitali ed è costantemente aggiornata, se del caso, per tutta la durata prevista del prodotto o per un periodo di cinque anni dopo la sua immissione sul mercato, a seconda di quale sia il periodo più breve.

3. Per i prodotti con elementi digitali di cui all'articolo 8 e all'articolo 24, paragrafo 4, che sono soggetti anche ad altri atti dell'Unione, è redatta un'unica documentazione tecnica contenente le informazioni di cui all'allegato V del presente regolamento e le informazioni richieste dai rispettivi atti dell'Unione.

4. La documentazione tecnica e la corrispondenza relativa a qualsiasi procedura di valutazione della conformità sono redatte in una delle lingue ufficiali dello Stato membro in cui è stabilito l'organismo notificato o in una lingua accettata da quest'ultimo.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 50 per integrare il presente regolamento con gli elementi da includere nella documentazione tecnica di cui all'allegato V, al fine di tenere conto degli sviluppi tecnologici e degli sviluppi riscontrati nel processo di attuazione del presente regolamento.

Articolo 24

Procedure di valutazione della conformità per prodotti con elementi digitali

1. Il fabbricante effettua una valutazione della conformità del prodotto con elementi digitali e dei processi messi in atto dal fabbricante per determinare se sono soddisfatti i requisiti essenziali di cui all'allegato I. Il fabbricante o il suo rappresentante autorizzato dimostra la conformità ai requisiti essenziali utilizzando una delle procedure seguenti:

   a) la procedura di controllo interno (basata sul modulo A) di cui all'allegato VI; o

   b) la procedura di esame UE del tipo (basata sul modulo B) di cui all'allegato VI, seguita dalla conformità al tipo UE basata sul controllo interno della produzione (basata sul modulo C) di cui all'allegato VI; o

   c) la valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'allegato VI.

2. Se per la valutazione della conformità del prodotto con elementi digitali critico di classe I di cui all'allegato III e dei processi messi in atto dal suo fabbricante ai requisiti essenziali di cui all'allegato I il fabbricante o il suo rappresentante autorizzato non ha applicato o ha applicato solo in parte norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza di cui all'articolo 18, o nel caso in cui non esistano tali norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza, il prodotto con elementi digitali in questione e i processi messi in atto dal fabbricante sono

sottoposti, per verificarne la conformità a tali requisiti essenziali, a una delle procedure seguenti:

a) procedura di esame UE del tipo (basata sul modulo B) di cui all'allegato VI, seguita dalla conformità al tipo UE basata sul controllo interno della produzione (basata sul modulo C) di cui all'allegato VI; o

b) la valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'allegato VI.

3. Se il prodotto è un prodotto con elementi digitali critico di classe II, come indicato nell'allegato III, il fabbricante o il suo rappresentante autorizzato dimostra la conformità ai requisiti essenziali di cui all'allegato I utilizzando una delle procedure seguenti:

a) la procedura di esame UE del tipo (basata sul modulo B) di cui all'allegato VI, seguita dalla conformità al tipo UE basata sul controllo interno della produzione (basata sul modulo C) di cui all'allegato VI; o

b) la valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'allegato VI.

4. I fabbricanti di prodotti con elementi digitali classificati come sistemi di cartelle cliniche elettroniche che rientrano nell'ambito di applicazione del regolamento [regolamento sullo spazio europeo dei dati sanitari] dimostrano la conformità ai requisiti essenziali di cui all'allegato I del presente regolamento utilizzando la procedura di valutazione della conformità pertinente prevista dal regolamento [capo III del regolamento sullo spazio europeo dei dati sanitari].

5. Gli organismi notificati tengono conto degli interessi e delle esigenze specifici delle piccole e medie imprese (PMI) quando definiscono le tariffe per le procedure di valutazione della conformità e riducono tali tariffe proporzionalmente agli interessi e alle esigenze specifici di tali imprese.

CAPO IV

NOTIFICA DEGLI ORGANISMI DI VALUTAZIONE DELLA CONFORMITÀ

Articolo 25

Notifica

Gli Stati membri notificano alla Commissione e agli altri Stati membri gli organismi di valutazione della conformità autorizzati a effettuare valutazioni della conformità a norma del presente regolamento.

Articolo 26

Autorità di notifica

1. Gli Stati membri designano 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, anche per quanto riguarda l'ottemperanza all'articolo 31.

2. Gli Stati membri possono decidere che la valutazione e il controllo di cui al paragrafo 1 siano eseguiti da un organismo nazionale di accreditamento ai sensi e in conformità del regolamento (CE) n. 765/2008.

Articolo 27

Requisiti relativi alle autorità di notifica

1. L'autorità di notifica è istituita in modo che non sorgano conflitti di interesse con gli organismi di valutazione della conformità.
2. L'autorità di notifica è organizzata e funziona in modo che siano salvaguardate l'obiettività e l'imparzialità delle sue attività.
3. L'autorità di notifica è organizzata in modo che ogni decisione relativa alla notifica di un organismo di valutazione della conformità sia adottata da persone competenti, diverse da quelle che hanno effettuato la valutazione.
4. L'autorità di notifica non offre e non fornisce attività svolte dagli organismi di valutazione della conformità o servizi di consulenza su base commerciale o concorrenziale.
5. L'autorità di notifica salvaguarda la riservatezza delle informazioni ottenute.
6. L'autorità di notifica ha a sua disposizione un numero di dipendenti competenti sufficiente per l'adeguata esecuzione dei suoi compiti.

Articolo 28

Obbligo di informazione a carico delle autorità di notifica

1. Gli Stati membri informano la Commissione delle loro procedure per la valutazione e la notifica degli organismi di valutazione della conformità e per il controllo degli organismi notificati, nonché di qualsiasi modifica delle stesse.
2. La Commissione rende pubbliche tali informazioni.

Articolo 29

Requisiti relativi agli organismi notificati

1. Ai fini della notifica, l'organismo di valutazione della conformità rispetta i requisiti di cui ai paragrafi da 2 a 12.
2. L'organismo di valutazione della conformità è istituito a norma della legge nazionale e ha personalità giuridica.
3. L'organismo di valutazione della conformità è un organismo terzo indipendente dall'organizzazione o dal prodotto che valuta.

   Un organismo appartenente a un'associazione d'imprese o a una federazione professionale che rappresenta imprese coinvolte nella progettazione, nello sviluppo, nella produzione, nella fornitura, nell'assemblaggio, nell'utilizzo o nella manutenzione di prodotti con elementi digitali che esso valuta può essere ritenuto un organismo di valutazione della conformità a condizione che ne siano dimostrate l'indipendenza e l'assenza di qualsiasi conflitto di interesse.
4. L'organismo di valutazione della conformità, i suoi alti dirigenti e il personale incaricato di svolgere i compiti di valutazione della conformità non sono né il

progettista, né lo sviluppatore, né il fabbricante, né il fornitore, né l'installatore, né l'acquirente, né il proprietario, né l'utilizzatore o il responsabile della manutenzione dei prodotti con elementi digitali che essi valutano, né il rappresentante autorizzato di uno di questi soggetti. Ciò non preclude l'uso di prodotti valutati che sono necessari per il funzionamento dell'organismo di valutazione della conformità né l'uso di tali prodotti a scopi personali.

L'organismo di valutazione della conformità, i suoi alti dirigenti e il personale incaricato di svolgere i compiti di valutazione della conformità non intervengono direttamente nella progettazione, nello sviluppo, nella produzione, nella commercializzazione, nell'installazione, nell'utilizzo o nella manutenzione di tali prodotti, né rappresentano i soggetti impegnati in tali attività. Essi non devono intraprendere alcuna attività che possa essere in conflitto con la loro indipendenza di giudizio o integrità riguardo alle attività di valutazione della conformità per cui sono notificati. Ciò vale in particolare per i servizi di consulenza.

Gli organismi di valutazione della conformità si accertano che le attività delle loro affiliate o dei loro subappaltatori non si ripercuotano sulla riservatezza, sull'obiettività o sull'imparzialità delle loro attività di valutazione della conformità.

5. Gli organismi di valutazione della conformità e il loro personale eseguono le operazioni di valutazione della conformità con il massimo dell'integrità professionale e con la competenza tecnica richiesta nel campo specifico e sono liberi da qualsivoglia pressione e incentivo, soprattutto di ordine finanziario, che possa influenzare il loro giudizio o i risultati delle loro attività di valutazione della conformità, in particolare da persone o gruppi di persone interessati ai risultati di tali attività.

6. L'organismo di valutazione della conformità è in grado di svolgere tutti i compiti di valutazione della conformità di cui all'allegato VI e per i quali è stato notificato, indipendentemente dal fatto che tali compiti siano eseguiti dall'organismo stesso o per suo conto e sotto la sua responsabilità.

   In ogni momento, per ogni procedura di valutazione della conformità e per ogni tipo o categoria di prodotti con elementi digitali per i quali è stato notificato, l'organismo di valutazione della conformità ha a sua disposizione:

   a) personale avente conoscenze tecniche ed esperienza sufficiente e appropriata per svolgere i compiti di valutazione della conformità;

   b) la descrizione delle procedure in base alle quali è svolta la valutazione della conformità, al fine di garantire la trasparenza e la capacità di riprodurre tali procedure. Esso dispone di politiche e procedure appropriate che distinguano i compiti che svolge in qualità di organismo notificato dalle altre attività;

   c) le procedure per svolgere le attività che tengono debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura, del grado di complessità della tecnologia del prodotto in questione e della natura di massa o seriale del processo produttivo.

   Esso dispone dei mezzi necessari per eseguire in modo appropriato i compiti tecnici e amministrativi connessi alle attività di valutazione della conformità e ha accesso a tutti gli strumenti o impianti occorrenti.

7. Il personale responsabile dell'esecuzione delle attività di valutazione della conformità dispone di quanto segue:

a) una formazione tecnica e professionale solida che includa tutte le attività di valutazione della conformità per cui l'organismo di valutazione della conformità è stato notificato;

b) soddisfacenti conoscenze dei requisiti relativi alle valutazioni che esegue e un'adeguata autorità per eseguire tali valutazioni;

c) una conoscenza e una comprensione adeguate dei requisiti essenziali, delle norme armonizzate applicabili e delle disposizioni pertinenti della normativa di armonizzazione dell'Unione, nonché dei suoi atti di esecuzione;

d) la capacità di redigere certificati, registri e relazioni atti a dimostrare che le valutazioni sono state eseguite.

8. È garantita l'imparzialità degli organismi di valutazione della conformità, dei loro alti dirigenti e del personale addetto alle valutazioni.

La remunerazione degli alti dirigenti e del personale addetto alle valutazioni di un organismo di valutazione della conformità non dipende dal numero di valutazioni eseguite o dai risultati di tali valutazioni.

9. Gli organismi di valutazione della conformità sottoscrivono un contratto di assicurazione per la responsabilità civile, a meno che detta responsabilità non sia direttamente coperta dallo Stato a norma del diritto nazionale o che lo Stato membro stesso non sia direttamente responsabile della valutazione della conformità.

10. Il personale dell'organismo di valutazione della conformità è tenuto al segreto professionale per tutto ciò di cui viene a conoscenza nell'esercizio delle sue funzioni a norma dell'allegato VI o di qualsiasi disposizione esecutiva di diritto interno, tranne nei confronti delle autorità di vigilanza del mercato dello Stato membro in cui esercita le sue attività. Sono tutelati i diritti di proprietà. L'organismo di valutazione della conformità dispone di procedure documentate che garantiscono la conformità al presente paragrafo.

11. Gli organismi di valutazione della conformità partecipano alle attività di normazione pertinenti e alle attività del gruppo di coordinamento degli organismi notificati istituito a norma dell'articolo 40, o garantiscono che il loro personale addetto alle valutazioni ne sia informato, e applicano come guida generale le decisioni e i documenti amministrativi prodotti da tale gruppo.

12. Gli organismi di valutazione della conformità operano secondo modalità e condizioni coerenti, eque e ragionevoli, tenendo conto in particolare degli interessi delle PMI in relazione alle tariffe.

Articolo 30

Presunzione di conformità degli organismi notificati

Qualora dimostri la propria conformità ai criteri stabiliti nelle pertinenti norme armonizzate o in parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, un organismo di valutazione della conformità è considerato conforme ai requisiti di cui all'articolo 29 nella misura in cui le norme applicabili armonizzate contemplano tali requisiti.

Articolo 31

Affiliate e subappaltatori degli organismi notificati

1. L'organismo notificato, qualora subappalti compiti specifici connessi alla valutazione della conformità oppure ricorra a un'affiliata, garantisce che il subappaltatore o l'affiliata soddisfi i requisiti di cui all'articolo 29 e ne informa l'autorità di notifica.

2. L'organismo notificato si assume la completa responsabilità dei compiti eseguiti dai subappaltatori o dalle affiliate, ovunque siano stabiliti.

3. Le attività possono essere subappaltate o eseguite da un'affiliata solo con il consenso del fabbricante.

4. Gli organismi notificati tengono a disposizione dell'autorità di notifica i documenti pertinenti riguardanti la valutazione delle qualifiche del subappaltatore o dell'affiliata e il lavoro da essi eseguito a norma del presente regolamento.

Articolo 32

Domanda di notifica

1. L'organismo di valutazione della conformità presenta una domanda di notifica all'autorità di notifica dello Stato membro in cui è stabilito.

2. Tale domanda è corredata di una descrizione delle attività di valutazione della conformità, della procedura o delle procedure di valutazione della conformità e del prodotto o dei prodotti per i quali l'organismo dichiara di essere competente, nonché, se disponibile, di un certificato di accreditamento rilasciato da un organismo nazionale di accreditamento che attesti che l'organismo di valutazione della conformità è conforme ai requisiti di cui all'articolo 29.

3. Qualora l'organismo di valutazione della conformità non possa fornire un certificato di accreditamento, esso fornisce all'autorità di notifica tutte le prove documentali necessarie per la verifica, il riconoscimento e il controllo periodico della sua conformità ai requisiti di cui all'articolo 29.

Articolo 33

Procedura di notifica

1. Le autorità di notifica possono notificare solo gli organismi di valutazione della conformità che soddisfino i requisiti di cui all'articolo 29.

2. L'autorità di notifica informa la Commissione e gli altri Stati membri utilizzando il sistema informativo NANDO (*New Approach Notified and Designated Organisations*) sviluppato e gestito dalla Commissione.

3. La notifica include tutti i dettagli riguardanti le attività di valutazione della conformità, il modulo o i moduli di valutazione della conformità e il prodotto o i prodotti interessati, nonché la relativa attestazione di competenza.

4. Qualora una notifica non sia basata su un certificato di accreditamento di cui all'articolo 32, paragrafo 2, l'autorità di notifica fornisce alla Commissione e agli altri Stati membri le prove documentali che attestino la competenza dell'organismo di valutazione della conformità nonché le disposizioni predisposte per fare in modo che tale organismo sia controllato periodicamente e continui a soddisfare i requisiti di cui all'articolo 29.

5. L'organismo interessato può eseguire le attività di un organismo notificato solo se non sono sollevate obiezioni da parte della Commissione o degli altri Stati membri

entro due settimane dalla notifica, qualora sia usato un certificato di accreditamento, o entro due mesi dalla notifica qualora non sia usato un accreditamento.

Solo tale organismo è considerato un organismo notificato ai fini del presente regolamento.

6. Alla Commissione e agli altri Stati membri sono comunicate eventuali modifiche di rilievo riguardanti la notifica.

Articolo 34

Numeri di identificazione ed elenchi degli organismi notificati

1. La Commissione attribuisce un numero di identificazione a ciascun organismo notificato.

Essa assegna un numero unico anche se l'organismo è notificato a norma di diversi atti dell'Unione.

2. La Commissione mette a disposizione del pubblico l'elenco degli organismi notificati a norma del presente regolamento, inclusi i numeri di identificazione loro assegnati e le attività per le quali sono stati notificati.

La Commissione provvede affinché l'elenco sia tenuto aggiornato.

Articolo 35

Modifiche delle notifiche

1. Qualora accerti o sia informata che un organismo notificato non è più conforme ai requisiti di cui all'articolo 29, o non adempie ai suoi obblighi, l'autorità di notifica limita, sospende o ritira la notifica, a seconda dei casi, in funzione della gravità del mancato rispetto di tali requisiti o dell'inadempimento di tali obblighi. Essa ne informa immediatamente la Commissione e gli altri Stati membri.

2. In caso di limitazione, sospensione o ritiro della notifica, oppure di cessazione dell'attività dell'organismo notificato, lo Stato membro notificante adotta le misure appropriate per garantire che le pratiche di tale organismo siano evase da un altro organismo notificato o siano messe a disposizione delle autorità di notifica e di vigilanza del mercato responsabili, su loro richiesta.

Articolo 36

Contestazione della competenza degli organismi notificati

1. La Commissione indaga su tutti i casi in cui abbia dubbi o siano portati alla sua attenzione dubbi sulla competenza di un organismo notificato o sulla continua ottemperanza di un organismo notificato ai requisiti e alle responsabilità cui è sottoposto.

2. Lo Stato membro notificante fornisce alla Commissione, su richiesta, tutte le informazioni relative alla base della notifica o del mantenimento della competenza dell'organismo in questione.

3. La Commissione garantisce la riservatezza di tutte le informazioni sensibili raccolte nel corso delle sue indagini.

4. La Commissione, qualora accerti che un organismo notificato non soddisfa o non soddisfa più i requisiti per la sua notifica, ne informa lo Stato membro notificante e chiede a quest'ultimo di adottare le misure correttive necessarie, incluso all'occorrenza il ritiro della notifica.

Articolo 37

Obblighi operativi degli organismi notificati

1. Gli organismi notificati eseguono le valutazioni della conformità conformemente alle procedure di valutazione della conformità di cui all'articolo 24 e all'allegato VI.

2. Le valutazioni della conformità sono eseguite in modo proporzionato, evitando oneri inutili per gli operatori economici. Gli organismi di valutazione della conformità svolgono le loro attività tenendo debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura, del grado di complessità della tecnologia del prodotto in questione e della natura di massa o seriale del processo produttivo.

3. Gli organismi notificati rispettano tuttavia il grado di rigore e il livello di tutela necessari per la conformità del prodotto alle disposizioni del regolamento.

4. Se un organismo notificato accerta che un fabbricante non ha rispettato i requisiti di cui all'allegato I o alle corrispondenti norme armonizzate o specifiche comuni di cui all'articolo 19, chiede a tale fabbricante di adottare le misure correttive del caso e non rilascia un certificato di conformità.

5. Qualora nel corso del monitoraggio della conformità successivo al rilascio di un certificato un organismo notificato rilevi che un prodotto non è più conforme ai requisiti stabiliti dal presente regolamento, esso chiede al fabbricante di adottare le misure correttive del caso e all'occorrenza sospende o ritira il certificato.

6. Qualora non siano adottate misure correttive o queste ultime non producano il risultato richiesto, l'organismo notificato limita, sospende o ritira i certificati, a seconda dei casi.

Articolo 38

Obbligo di informazione a carico degli organismi notificati

1. Gli organismi notificati informano l'autorità di notifica:

   a) di qualunque rifiuto, limitazione, sospensione o ritiro di un certificato;

   b) di qualunque circostanza che possa influire sull'ambito e sulle condizioni della notifica;

   c) di eventuali richieste di informazioni che abbiano ricevuto dalle autorità di vigilanza del mercato, in relazione ad attività di valutazione della conformità;

   d) su richiesta, delle attività di valutazione della conformità eseguite nell'ambito della loro notifica e di qualsiasi altra attività, incluse quelle transfrontaliere e relative al subappalto.

2. Gli organismi notificati forniscono agli altri organismi notificati a norma del presente regolamento, le cui attività di valutazione della conformità sono simili e hanno come oggetto gli stessi prodotti, informazioni pertinenti su questioni relative ai risultati negativi e, su richiesta, ai risultati positivi delle valutazioni della conformità.

Articolo 39

Scambio di esperienze

La Commissione provvede all'organizzazione di uno scambio di esperienze tra le autorità nazionali degli Stati membri responsabili della politica di notifica.

Articolo 40

Coordinamento degli organismi notificati

1. La Commissione garantisce l'istituzione e il corretto funzionamento di un coordinamento e una cooperazione appropriati tra organismi notificati sotto forma di un gruppo intersettoriale di organismi notificati.

2. Gli Stati membri garantiscono che gli organismi da essi notificati partecipino al lavoro di tale gruppo, direttamente o mediante rappresentanti designati.

CAPO V

VIGILANZA DEL MERCATO E APPLICAZIONE DELLE NORME

Articolo 41

Vigilanza del mercato e controllo dei prodotti con elementi digitali nel mercato dell'Unione

1. Il regolamento (UE) 2019/1020 si applica ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento.

2. Ciascuno Stato membro designa una o più autorità di vigilanza del mercato al fine di garantire l'efficace attuazione del presente regolamento. Gli Stati membri possono designare un'autorità già esistente o una nuova autorità che agisca come autorità di vigilanza del mercato ai fini del presente regolamento.

3. Le autorità di vigilanza del mercato collaborano, se pertinente, con le autorità nazionali di certificazione della cibersicurezza designate a norma dell'articolo 58 del regolamento (UE) 2019/881 e procedono regolarmente a scambi di informazioni. Per quanto riguarda la sorveglianza dell'attuazione degli obblighi di segnalazione di cui all'articolo 11 del presente regolamento, le autorità di vigilanza del mercato designate collaborano con l'ENISA.

4. Le autorità di vigilanza del mercato cooperano, se pertinente, con altre autorità di vigilanza del mercato designate sulla base di altre normative di armonizzazione dell'Unione per altri prodotti e procedono regolarmente a scambi di informazioni.

5. Le autorità di vigilanza del mercato collaborano, all'occorrenza, con le autorità preposte alla vigilanza del diritto dell'Unione in materia di protezione dei dati. Rientra in tale cooperazione la comunicazione a dette autorità di qualsiasi risultanza pertinente per l'esercizio delle loro competenze, anche nell'ambito della fornitura di orientamenti e consulenze a norma del paragrafo 8 del presente articolo, se tali orientamenti e consulenze riguardano il trattamento dei dati personali.

   Le autorità preposte alla vigilanza del diritto dell'Unione in materia di protezione dei dati hanno il potere di richiedere qualsiasi documentazione creata o conservata a norma del presente regolamento e di accedervi, qualora l'accesso a tale documentazione sia necessario per lo svolgimento dei loro compiti. Esse informano

le autorità di vigilanza del mercato designate dello Stato membro interessato di tale richiesta.

6. Gli Stati membri garantiscono che le autorità di vigilanza del mercato designate dispongano di risorse finanziarie e umane adeguate per svolgere i loro compiti a norma del presente regolamento.

7. La Commissione agevola lo scambio di esperienze tra le autorità di vigilanza del mercato designate.

8. Le autorità di vigilanza del mercato possono fornire agli operatori economici orientamenti e consulenza sull'attuazione del presente regolamento, con il sostegno della Commissione.

9. Le autorità di vigilanza del mercato riferiscono annualmente alla Commissione in merito ai risultati delle pertinenti attività di vigilanza del mercato. Le autorità di vigilanza del mercato designate comunicano senza indugio alla Commissione e alle pertinenti autorità nazionali garanti della concorrenza qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per l'applicazione del diritto dell'Unione in materia di concorrenza.

10. Per quanto riguarda i prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento classificati come sistemi di IA ad alto rischio conformemente all'articolo [articolo 6] del regolamento [regolamento sull'IA], le autorità di vigilanza del mercato designate ai fini del regolamento [regolamento sull'IA] sono le autorità responsabili delle attività di vigilanza del mercato previste dal presente regolamento. Le autorità di vigilanza del mercato designate a norma del regolamento [regolamento sull'IA] cooperano, all'occorrenza, con le autorità di vigilanza del mercato designate a norma del presente regolamento e, per quanto riguarda la sorveglianza dell'attuazione degli obblighi di segnalazione a norma dell'articolo 11, con l'ENISA. Le autorità di vigilanza del mercato designate a norma del regolamento [regolamento sull'IA] informano in particolare le autorità di vigilanza del mercato designate a norma del presente regolamento di qualsiasi risultanza pertinente per lo svolgimento dei loro compiti in relazione all'attuazione del presente regolamento.

11. Per l'applicazione uniforme del presente regolamento è istituito un apposito gruppo di cooperazione amministrativa (ADCO) a norma dell'articolo 30, paragrafo 2, del regolamento (UE) 2019/1020. Tale ADCO è composto da rappresentanti delle autorità di vigilanza del mercato designate e, se del caso, da rappresentanti degli uffici unici di collegamento.

Articolo 42

Accesso ai dati e documentazione

Se necessario per valutare la conformità dei prodotti con elementi digitali e dei processi messi in atto dai loro fabbricanti ai requisiti essenziali di cui all'allegato I e su richiesta motivata, alle autorità di vigilanza del mercato è consentito l'accesso ai dati necessari per valutare la progettazione, lo sviluppo, la produzione e la gestione delle vulnerabilità di tali prodotti, compresa la relativa documentazione interna del rispettivo operatore economico.

Articolo 43

Procedura a livello nazionale relativa ai prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo

1. Qualora l'autorità di vigilanza del mercato di uno Stato membro abbia motivi sufficienti per ritenere che un prodotto con elementi digitali, compresa la relativa gestione delle vulnerabilità, presenti un rischio di cibersicurezza significativo, essa effettua una valutazione del prodotto con elementi digitali interessato per quanto riguarda la sua conformità a tutti i requisiti di cui al presente regolamento. Gli operatori economici interessati cooperano, per quanto necessario, con l'autorità di vigilanza del mercato.

   Se, attraverso la valutazione, l'autorità di vigilanza del mercato conclude che il prodotto con elementi digitali non rispetta i requisiti di cui al presente regolamento, essa chiede senza indugio all'operatore interessato di adottare tutte le opportune misure correttive al fine di rendere il prodotto conforme ai suddetti requisiti oppure di ritirarlo o di richiamarlo dal mercato entro un termine ragionevole e proporzionato alla natura del rischio, a seconda dei casi.

   L'autorità di vigilanza del mercato informa di conseguenza l'organismo notificato pertinente. L'articolo 18 del regolamento (UE) 2019/1020 si applica alle opportune misure correttive.

2. Qualora ritenga che la non conformità non sia limitata al territorio nazionale, l'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri dei risultati della valutazione e delle azioni che ha chiesto all'operatore economico di intraprendere.

3. Il fabbricante garantisce che siano adottate tutte le opportune misure correttive nei confronti di tutti i prodotti con elementi digitali interessati che ha messo a disposizione sul mercato in tutta l'Unione.

4. Qualora il fabbricante di un prodotto con elementi digitali non adotti misure correttive adeguate entro il termine di cui al paragrafo 1, secondo comma, l'autorità di vigilanza del mercato adotta tutte le opportune misure provvisorie per vietare o limitare la messa a disposizione del prodotto sul suo mercato nazionale, per ritirarlo da tale mercato o per richiamarlo.

   Tale autorità informa senza indugio la Commissione e gli altri Stati membri di tali misure.

5. Le informazioni di cui al paragrafo 4 includono tutti i dettagli disponibili, soprattutto i dati necessari all'identificazione del prodotto con elementi digitali non conforme, la sua origine, la natura della presunta non conformità e i rischi connessi, la natura e la durata delle misure nazionali adottate, nonché gli argomenti espressi dall'operatore interessato. L'autorità di vigilanza del mercato indica in particolare se la non conformità sia dovuta a una o più delle cause seguenti:

   a) mancato rispetto dei requisiti essenziali di cui all'allegato I da parte del prodotto o dei processi messi in atto dal fabbricante;

   b) carenze nelle norme armonizzate, nei sistemi di certificazione della cibersicurezza o nelle specifiche comuni di cui all'articolo 18.

6. Le autorità di vigilanza del mercato degli Stati membri diverse dall'autorità di vigilanza del mercato dello Stato membro che ha avviato la procedura comunicano

senza indugio alla Commissione e agli altri Stati membri tutte le misure adottate, tutte le altre informazioni a loro disposizione sulla non conformità del prodotto interessato e, in caso di disaccordo con la misura nazionale notificata, le loro obiezioni.

7. Qualora, entro tre mesi dal ricevimento delle informazioni di cui al paragrafo 4, uno Stato membro o la Commissione non sollevino obiezioni contro la misura provvisoria adottata da uno Stato membro, tale misura è ritenuta giustificata. Ciò non pregiudica i diritti procedurali dell'operatore interessato in conformità dell'articolo 18 del regolamento (UE) 2019/1020.

8. Le autorità di vigilanza del mercato di tutti gli Stati membri garantiscono che siano adottate senza indugio adeguate misure restrittive in relazione al prodotto interessato, come il ritiro del prodotto dal loro mercato.

Articolo 44

Procedura di salvaguardia dell'Unione

1. Se entro tre mesi dal ricevimento della notifica di cui all'articolo 43, paragrafo 4, uno Stato membro solleva obiezioni contro la misura adottata da un altro Stato membro, o se la Commissione ritiene che la misura sia contraria alla normativa dell'Unione, la Commissione consulta senza indugio lo Stato membro interessato e l'operatore o gli operatori economici e valuta la misura nazionale. Sulla base dei risultati di tale valutazione, la Commissione decide se la misura nazionale sia giustificata o meno entro nove mesi dalla notifica di cui all'articolo 43, paragrafo 4, e notifica tale decisione allo Stato membro interessato.

2. Se la misura nazionale è ritenuta giustificata, tutti gli Stati membri adottano le misure necessarie a garantire che il prodotto con elementi digitali non conforme sia ritirato dal loro mercato e ne informano la Commissione. Se la misura nazionale è ritenuta ingiustificata, lo Stato membro interessato provvede a ritirarla.

3. Se la misura nazionale è ritenuta giustificata e la non conformità del prodotto con elementi digitali è attribuita a carenze nelle norme armonizzate, la Commissione applica la procedura di cui all'articolo 10 del regolamento (UE) n. 1025/2012.

4. Se la misura nazionale è ritenuta giustificata e la non conformità del prodotto con elementi digitali è attribuita a carenze in un sistema europeo di certificazione della cibersicurezza di cui all'articolo 18, la Commissione valuta se modificare o abrogare l'atto di esecuzione di cui all'articolo 18, paragrafo 4, che specifica la presunzione di conformità relativa a tale sistema di certificazione.

5. Se la misura nazionale è ritenuta giustificata e la non conformità del prodotto con elementi digitali è attribuita a carenze nelle specifiche comuni di cui all'articolo 19, la Commissione valuta se modificare o abrogare l'atto di esecuzione di cui all'articolo 19 che stabilisce tali specifiche comuni.

Articolo 45

Procedura a livello dell'UE relativa ai prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo

1. Se la Commissione ha motivi sufficienti per ritenere, anche sulla base delle informazioni fornite dall'ENISA, che un prodotto con elementi digitali che presenta un rischio di cibersicurezza significativo non sia conforme ai requisiti stabiliti nel

presente regolamento, può chiedere alle autorità di vigilanza del mercato competenti di effettuare una valutazione della conformità e di seguire le procedure di cui all'articolo 43.

2. In circostanze eccezionali che giustifichino un intervento immediato per preservare il buon funzionamento del mercato interno e qualora la Commissione abbia motivi sufficienti per ritenere che il prodotto di cui al paragrafo 1 continui a non essere conforme ai requisiti stabiliti dal presente regolamento e che non siano state adottate misure efficaci dalle autorità di vigilanza del mercato competenti, la Commissione può chiedere all'ENISA di effettuare una valutazione della conformità. La Commissione ne informa le autorità di vigilanza del mercato competenti. Gli operatori economici interessati cooperano, per quanto necessario, con l'ENISA.

3. Sulla base della valutazione dell'ENISA, la Commissione può decidere che è necessaria una misura correttiva o restrittiva a livello dell'Unione. A tal fine essa consulta senza indugio gli Stati membri interessati e l'operatore o gli operatori economici interessati.

4. Sulla base della consultazione di cui al paragrafo 3, la Commissione può adottare atti di esecuzione per decidere in merito alle misure correttive o restrittive a livello dell'Unione, tra cui l'ordine di ritiro dal mercato o il richiamo, entro un termine ragionevole, proporzionato alla natura del rischio. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 51, paragrafo 2.

5. La Commissione comunica immediatamente la decisione di cui al paragrafo 4 all'operatore o agli operatori economici interessati. Gli Stati membri attuano senza indugio gli atti di cui al paragrafo 4 e ne informano la Commissione.

6. I paragrafi da 2 a 5 si applicano per la durata della situazione eccezionale che ha giustificato l'intervento della Commissione e per tutto il tempo in cui il prodotto in questione non è reso conforme al presente regolamento.

Articolo 46

Prodotti con elementi digitali conformi che presentano un rischio di cibersicurezza significativo

1. Se, dopo aver effettuato una valutazione a norma dell'articolo 43, l'autorità di vigilanza del mercato di uno Stato membro ritiene che, sebbene conformi al presente regolamento, il prodotto con elementi digitali e i processi messi in atto dal fabbricante presentino un rischio di cibersicurezza significativo e comportino inoltre un rischio per la salute o la sicurezza delle persone, per la conformità agli obblighi previsti dal diritto dell'Unione o nazionale a tutela dei diritti fondamentali, per la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti utilizzando un sistema di informazione elettronico da parte di soggetti essenziali del tipo di cui [all'allegato I della direttiva XXX/XXXX (NIS2)] o per altri aspetti della tutela dell'interesse pubblico, essa chiede all'operatore interessato di adottare tutte le misure appropriate a far sì che il prodotto con elementi digitali e i processi messi in atto dal fabbricante interessato, all'atto dell'immissione sul mercato, non presentino più tale rischio oppure che il prodotto con elementi digitali sia ritirato dal mercato o richiamato entro un termine ragionevole, proporzionato alla natura del rischio.

2. Il fabbricante o altri operatori pertinenti garantiscono l'adozione di misure correttive nei confronti dei prodotti con elementi digitali interessati che hanno messo a

disposizione sul mercato in tutta l'Unione entro il termine stabilito dall'autorità di vigilanza del mercato dello Stato membro di cui al paragrafo 1.

3. Lo Stato membro informa immediatamente la Commissione e gli altri Stati membri in merito alle misure adottate a norma del paragrafo 1. Tali informazioni comprendono tutti i dettagli disponibili, segnatamente i dati necessari all'identificazione dei prodotti con elementi digitali interessati, l'origine e la catena di approvvigionamento di tali prodotti, la natura dei rischi connessi, nonché la natura e la durata delle misure nazionali adottate.

4. La Commissione avvia senza indugio consultazioni con gli Stati membri e l'operatore economico interessato e valuta le misure nazionali adottate. In base ai risultati della valutazione, la Commissione decide se la misura sia giustificata o no e propone, all'occorrenza, misure appropriate.

5. La Commissione trasmette la decisione agli Stati membri.

6. Se ha motivi sufficienti per ritenere, anche sulla base delle informazioni fornite dall'ENISA, che un prodotto con elementi digitali, sebbene conforme al presente regolamento, presenti i rischi di cui al paragrafo 1, la Commissione può chiedere all'autorità o alle autorità di vigilanza del mercato competenti di effettuare una valutazione della conformità e di seguire le procedure di cui all'articolo 43 e al presente articolo, paragrafi 1, 2 e 3.

7. In circostanze eccezionali che giustifichino un intervento immediato per preservare il buon funzionamento del mercato interno e qualora la Commissione abbia motivi sufficienti per ritenere che il prodotto di cui al paragrafo 6 continui a presentare i rischi di cui al paragrafo 1 e che le autorità nazionali di vigilanza del mercato competenti non abbiano adottato misure efficaci, la Commissione può chiedere all'ENISA di effettuare una valutazione dei rischi presentati da tale prodotto e ne informa le autorità di vigilanza del mercato competenti. Gli operatori economici interessati cooperano, per quanto necessario, con l'ENISA.

8. Sulla base della valutazione dell'ENISA di cui al paragrafo 7, la Commissione può stabilire che è necessaria una misura correttiva o restrittiva a livello dell'Unione. A tal fine essa consulta senza indugio gli Stati membri interessati e l'operatore o gli operatori interessati.

9. Sulla base della consultazione di cui al paragrafo 8, la Commissione può adottare atti di esecuzione per decidere in merito alle misure correttive o restrittive a livello dell'Unione, tra cui l'ordine di ritiro dal mercato o il richiamo, entro un termine ragionevole, proporzionato alla natura del rischio. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 51, paragrafo 2.

10. La Commissione comunica immediatamente la decisione di cui al paragrafo 9 all'operatore o agli operatori interessati. Gli Stati membri attuano tali atti senza indugio e ne informano la Commissione.

11. I paragrafi da 6 a 10 si applicano per la durata della situazione eccezionale che ha giustificato l'intervento della Commissione e per tutto il tempo in cui il prodotto in questione continua a presentare i rischi di cui al paragrafo 1.

Articolo 47

Non conformità formale

1. Un'autorità di vigilanza del mercato di uno Stato membro che giunga a una delle conclusioni riportate di seguito chiede al fabbricante interessato di porre fine alla non conformità contestata:

   a) la marcatura di conformità è stata apposta in violazione degli articoli 21 e 22;

   b) la marcatura di conformità non è stata apposta;

   c) la dichiarazione di conformità UE non è stata redatta;

   d) la dichiarazione di conformità UE non è stata redatta correttamente;

   e) il numero di identificazione dell'organismo notificato coinvolto nella procedura di valutazione della conformità, ove applicabile, non è stato apposto;

   f) la documentazione tecnica non è disponibile o non è completa.

2. Se la non conformità di cui al paragrafo 1 permane, lo Stato membro interessato adotta tutte le misure appropriate per limitare o proibire la messa a disposizione sul mercato del prodotto con elementi digitali o per garantire che sia richiamato o ritirato dal mercato.

Articolo 48

Attività congiunte delle autorità di vigilanza del mercato

1. Le autorità di vigilanza del mercato possono stipulare accordi con altre autorità competenti per la realizzazione di attività congiunte volte a garantire la cibersicurezza e la tutela dei consumatori in relazione a specifici prodotti con elementi digitali immessi o messi a disposizione sul mercato, in particolare i prodotti che spesso presentano rischi di cibersicurezza.

2. La Commissione o l'ENISA possono proporre attività congiunte di verifica della conformità al presente regolamento che saranno svolte dalle autorità di vigilanza del mercato sulla base di indicazioni o informazioni riguardanti la potenziale non conformità, in diversi Stati membri, di prodotti che rientrano nell'ambito di applicazione del presente regolamento ai requisiti stabiliti da quest'ultimo.

3. Le autorità di vigilanza del mercato e la Commissione, se del caso, garantiscono che l'accordo sullo svolgimento di attività congiunte non comporti una concorrenza sleale tra gli operatori economici e non pregiudichi l'obiettività, l'indipendenza e l'imparzialità delle parti dell'accordo.

4. Un'autorità di vigilanza del mercato ha facoltà di utilizzare qualsivoglia informazione derivante dalle attività svolte nell'ambito di un'indagine da essa condotta.

5. L'autorità di vigilanza del mercato competente e la Commissione, se del caso, mettono a disposizione del pubblico l'accordo sulle attività congiunte, compresi i nomi delle parti coinvolte.

Articolo 49

Indagini a tappeto

1. Le autorità di vigilanza del mercato possono decidere di condurre simultaneamente azioni di controllo coordinate ("indagini a tappeto") di particolari prodotti con elementi digitali o relative categorie per verificarne la conformità con il presente regolamento o per individuare violazioni.

2. Salvo diverso accordo tra le autorità di vigilanza del mercato coinvolte, le indagini a tappeto sono coordinate dalla Commissione. Il coordinatore dell'indagine a tappeto può, se del caso, mettere a disposizione del pubblico i risultati aggregati.

3. L'ENISA può individuare, nell'esecuzione dei suoi compiti, anche sulla base delle notifiche ricevute conformemente all'articolo 11, paragrafi 1 e 2, categorie di prodotti per le quali possono essere organizzate indagini a tappeto. La proposta di indagini a tappeto è sottoposta al potenziale coordinatore di cui al paragrafo 2 per essere esaminata dalle autorità di vigilanza del mercato.

4. Nello svolgere indagini a tappeto, le autorità di vigilanza del mercato coinvolte possono usare i poteri di indagine di cui agli articoli da 41 a 47 e gli altri poteri a esse conferiti dal diritto nazionale.

5. Le autorità di vigilanza del mercato possono invitare i funzionari della Commissione e altre persone di accompagnamento autorizzate dalla Commissione a partecipare alle indagini a tappeto.

CAPO VI

DELEGA DI POTERE E PROCEDURA DI COMITATO

Articolo 50

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 2, paragrafo 4, all'articolo 6, paragrafi 2, 3 e 5, all'articolo 20, paragrafo 5, e all'articolo 23, paragrafo 5, è conferito alla Commissione.

3. La delega di potere di cui all'articolo 2, paragrafo 4, all'articolo 6, paragrafi 2, 3 e 5, all'articolo 20, paragrafo 5, e all'articolo 23, paragrafo 5, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 2, paragrafo 4, dell'articolo 6, paragrafi 2, 3 e 5, dell'articolo 20, paragrafo 5, e dell'articolo 23, paragrafo 5, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 51

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

3. Laddove il parere del comitato debba essere ottenuto con procedura scritta, questa procedura si conclude senza esito quando, entro il termine per la formulazione del parere, il presidente del comitato decida in tal senso o un membro del comitato lo richieda.

CAPO VII

RISERVATEZZA E SANZIONI

Articolo 52

Riservatezza

1. Tutte le parti che partecipano all'applicazione del presente regolamento rispettano la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività in modo da tutelare, in particolare:

   a) i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali di una persona fisica o giuridica, compreso il codice sorgente, tranne i casi cui si applica l'articolo 5 della direttiva 2016/943 del Parlamento europeo e del Consiglio[24];

   b) l'efficace attuazione del presente regolamento, in particolare per quanto riguarda ispezioni, indagini o audit;

   c) gli interessi di sicurezza pubblica e nazionale;

   d) l'integrità del procedimento penale o amministrativo.

2. Fatto salvo il paragrafo 1, le informazioni scambiate in via riservata tra le autorità di vigilanza del mercato e tra queste ultime e la Commissione non sono divulgate senza il preventivo accordo dell'autorità di vigilanza del mercato dalla quale tali informazioni provengono.

3. I paragrafi 1 e 2 non pregiudicano i diritti e gli obblighi della Commissione, degli Stati membri e degli organismi notificati in materia di scambio delle informazioni e di diffusione degli avvisi di sicurezza, né gli obblighi delle persone interessate di fornire informazioni a norma del diritto penale degli Stati membri.

4. La Commissione e gli Stati membri possono scambiare, ove necessario, informazioni sensibili con le autorità competenti dei paesi terzi con i quali abbiano concluso

[24] Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti (GU L 157 del 15.6.2016, pag. 1).

accordi di riservatezza, bilaterali o multilaterali, che garantiscano un livello di protezione adeguato.

Articolo 53

Sanzioni

1. Gli Stati membri fissano le norme sulle sanzioni applicabili in caso di violazione del presente regolamento da parte degli operatori economici e prendono tutti i provvedimenti necessari per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive.

2. Gli Stati membri notificano tali norme e misure alla Commissione, senza indugio, e provvedono poi a dare immediata notifica delle eventuali modifiche successive.

3. La non conformità ai requisiti essenziali di cibersicurezza di cui all'allegato I e agli obblighi di cui agli articoli 10 e 11 è soggetta a sanzioni amministrative pecuniarie fino a 15 000 000 di EUR o, se l'autore del reato è un'impresa, fino al 2,5 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

4. La non conformità a qualsiasi altro obbligo previsto dal presente regolamento è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 di EUR o, se l'autore del reato è un'impresa, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

5. La fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità di vigilanza del mercato è soggetta a sanzioni amministrative pecuniarie fino a 5 000 000 di EUR o, se l'autore del reato è un'impresa, fino all'1 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

6. Nel decidere l'importo della sanzione amministrativa pecuniaria in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e si tiene quanto segue in debita considerazione:

   a) la natura, la gravità e la durata della violazione e delle sue conseguenze;

   b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per una violazione analoga;

   c) le dimensioni e la quota di mercato dell'operatore che ha commesso la violazione.

7. Le autorità di vigilanza del mercato che applicano sanzioni amministrative pecuniarie condividono tale informazione con le autorità di vigilanza del mercato di altri Stati membri mediante il sistema di informazione e comunicazione di cui all'articolo 34 del regolamento (UE) 2019/1020.

8. Ciascuno Stato membro può prevedere regole che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

9. A seconda dell'ordinamento giuridico degli Stati membri, le regole in materia di sanzioni amministrative pecuniarie possono essere applicate in modo tale che le sanzioni pecuniarie siano inflitte dai tribunali nazionali competenti o da altri organismi in base alle competenze stabilite a livello nazionale in tali Stati membri. L'applicazione di tali regole in tali Stati membri ha effetto equivalente.

10. Le sanzioni amministrative pecuniarie possono essere inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta a qualsiasi altra misura correttiva o restrittiva applicata dalle autorità di vigilanza del mercato per la stessa violazione.

CAPO VIII

DISPOSIZIONI TRANSITORIE E FINALI

Articolo 54

Modifica del regolamento (UE) 2019/1020

Nell'allegato I del regolamento (UE) 2019/1020 è aggiunto il seguente punto:

"71. [regolamento XXX][legge sulla ciberresilienza]".

Articolo 55

Disposizioni transitorie

1. I certificati di esame UE del tipo e le decisioni di approvazione rilasciati in relazione ai requisiti di cibersicurezza per i prodotti con elementi digitali soggetti ad altra normativa di armonizzazione dell'Unione rimangono validi fino al [42 mesi dopo la data di entrata in vigore del presente regolamento], a meno che non scadano prima di tale data o non sia altrimenti disposto in altre normative dell'Unione, nel qual caso rimangono validi come indicato in tali normative.
2. I prodotti con elementi digitali immessi sul mercato prima del [data di applicazione del presente regolamento di cui all'articolo 57] sono soggetti ai requisiti del presente regolamento solo se, a decorrere da tale data, tali prodotti sono soggetti a modifiche sostanziali nella loro progettazione o finalità prevista.
3. In deroga al paragrafo 2, gli obblighi di cui all'articolo 11 si applicano a tutti i prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento e che sono stati immessi sul mercato prima del [data di applicazione del presente regolamento di cui all'articolo 57].

Articolo 56

Valutazione e riesame

Entro [36 mesi dalla data di applicazione del presente regolamento] e successivamente ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione sulla valutazione e sul riesame del presente regolamento. Tale relazione è pubblicata.

Articolo 57

Entrata in vigore e applicazione

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Esso si applica a partire dal [24 mesi dopo la data della sua entrata in vigore]. Tuttavia l'articolo 11 si applica a partire dal [12 mesi dopo la data di entrata in vigore del presente regolamento].

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati

1.3. La proposta/iniziativa riguarda:

1.4. Obiettivi

1.4.1. Obiettivi generali

1.4.2. Obiettivi specifici

1.4.3. Risultati e incidenza previsti

1.4.4. Indicatori di prestazione

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.

1.5.3. Insegnamenti tratti da esperienze analoghe

1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti

1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione

1.6. Durata e incidenza finanziaria della proposta/iniziativa

1.7. Modalità di gestione previste

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistema di gestione e di controllo

2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli

2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti

3.2.1. Sintesi dell'incidenza prevista sugli stanziamenti operativi

3.2.2. Risultati previsti finanziati con gli stanziamenti operativi

3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (legge sulla ciberresilienza)

1.2. Settore/settori interessati

Reti di comunicazione, contenuti e tecnologie

1.3. La proposta/iniziativa riguarda:

× **una nuova azione**

☐ **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[37]

☐ **la proroga di un'azione esistente**

☐ **la fusione o il riorientamento di una o più azioni verso un'altra/una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivi generali

La proposta ha due obiettivi principali che mirano a garantire il corretto funzionamento del mercato interno: 1) **creare le condizioni per lo sviluppo di prodotti con elementi digitali sicuri**, garantendo che i prodotti hardware e software siano immessi sul mercato con un minor numero di vulnerabilità e che i fabbricanti prendano la sicurezza in seria considerazione durante l'intero ciclo di vita di un prodotto; e 2) **creare le condizioni che consentano agli utilizzatori di tenere conto della cibersicurezza nella scelta e nell'utilizzo dei prodotti con elementi digitali**.

1.4.2. Obiettivi specifici

Per la proposta sono stati definiti **quattro obiettivi specifici**: i) 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; ii) garantire un quadro coerente in materia di cibersicurezza, facilitando la conformità per i produttori di hardware e software; iii) migliorare la trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali e iv) consentire alle imprese e ai consumatori di utilizzarli in modo sicuro.

Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

La proposta apporterebbe benefici significativi ai vari portatori di interessi. Per le imprese, eviterebbe norme di sicurezza divergenti per i prodotti con elementi digitali, ridurrebbe i costi di conformità alla relativa normativa in materia di cibersicurezza e diminuirebbe il numero di incidenti informatici, i costi di gestione degli incidenti e i danni alla reputazione. Per l'intera UE si stima che l'iniziativa potrebbe comportare

[37] A norma dell'articolo 58, paragrafo 2, lettera a) o b), del regolamento finanziario.

una riduzione dei costi degli incidenti che interessano le imprese di circa 180-290 miliardi di EUR all'anno[38]. Determinerebbe inoltre un aumento del fatturato grazie alla diffusione della domanda di prodotti con elementi digitali e migliorerebbe la reputazione delle imprese a livello mondiale, portando a un aumento della domanda anche da fuori l'UE. Per gli utilizzatori l'opzione prescelta aumenterebbe la trasparenza delle proprietà di sicurezza e faciliterebbe l'uso dei prodotti con elementi digitali. I consumatori e i cittadini beneficerebbero inoltre di una migliore tutela dei loro diritti fondamentali, come la protezione della vita privata e dei dati.

Al contempo la proposta genererebbe costi di conformità e di applicazione per le imprese, gli organismi notificati e le autorità pubbliche, comprese le autorità di accreditamento e di vigilanza del mercato. Per gli sviluppatori di software e i fabbricanti di hardware si aggiungeranno costi diretti di conformità per i nuovi requisiti di sicurezza, la valutazione della conformità, gli obblighi di documentazione e di segnalazione, che porteranno a costi aggregati di conformità pari a circa 29 miliardi di EUR per un valore di mercato stimato di 1 485 miliardi di EUR di fatturato[39]. Gli utilizzatori, compresi gli utilizzatori commerciali, i consumatori e i cittadini, possono incorrere in un aumento dei prezzi dei prodotti con elementi digitali. Tuttavia tale aumento dovrebbe essere considerato alla luce dei benefici significativi descritti in precedenza.

1.4.3. Indicatori di prestazione

Precisare gli indicatori con cui monitorare progressi e risultati

Per verificare se i fabbricanti migliorano la sicurezza dei loro prodotti con elementi digitali fin dalla fase di progettazione e sviluppo e durante l'intero ciclo di vita di tali prodotti, si potrebbero prendere in considerazione diversi indicatori. Tra questi potrebbero figurare il numero di incidenti di rilievo nell'Unione causati da vulnerabilità, la percentuale di fabbricanti di hardware e software che seguono un ciclo di vita di sviluppo sicuro sistematico, un'analisi qualitativa della sicurezza dei prodotti con elementi digitali, una valutazione quantitativa e qualitativa delle banche dati delle vulnerabilità, la frequenza delle patch di sicurezza messe a disposizione dai fabbricanti o il numero medio di giorni che intercorrono tra l'individuazione delle vulnerabilità e la fornitura delle patch di sicurezza.

Un indicatore relativo a un quadro coerente in materia di cibersicurezza potrebbe essere l'assenza di una normativa nazionale mirata in materia di cibersicurezza specifica per prodotto.

Un indicatore relativo a una maggiore trasparenza delle proprietà di sicurezza dei prodotti con elementi digitali potrebbe essere la percentuale di prodotti con elementi digitali che sono consegnati corredati di informazioni sulle proprietà di sicurezza. Inoltre la percentuale di prodotti con elementi digitali che sono consegnati corredati di istruzioni sull'utilizzo sicuro potrebbe essere impiegata come indicatore del fatto che le organizzazioni e i consumatori sono messi nelle condizioni di utilizzare i prodotti con elementi digitali in modo sicuro.

---

38 Cfr. [documento di lavoro dei servizi della Commissione relativo alla relazione sulla valutazione d'impatto che accompagna il regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali].

39 Cfr. [documento di lavoro dei servizi della Commissione relativo alla relazione sulla valutazione d'impatto che accompagna il regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali].

Per quanto riguarda il monitoraggio dell'impatto del regolamento, si prenderanno in considerazione alcuni indicatori che saranno valutati dalla Commissione, se del caso con il sostegno dell'ENISA. A seconda dell'obiettivo operativo da raggiungere, alcuni degli indicatori di monitoraggio in base ai quali valutare il successo dei requisiti orizzontali di cibersicurezza sono indicati di seguito.

Per valutare il livello di cibersicurezza dei prodotti con elementi digitali:

- statistiche e analisi qualitative sugli incidenti che hanno interessato prodotti con elementi digitali e sul modo in cui sono stati gestiti. Questi dati potrebbero essere raccolti e valutati dalla Commissione con il sostegno dell'ENISA;

- registri di vulnerabilità note e analisi di come sono state gestite. Tale analisi potrebbe essere condotta dall'ENISA, sulla base della banca dati europea delle vulnerabilità istituita a norma della [direttiva XXX/XXXX (NIS2)];

- indagini tra i fabbricanti di hardware e software per monitorare i progressi.

Per valutare il livello di informazioni sulle caratteristiche di sicurezza, l'assistenza di sicurezza, la fine del ciclo di vita e il dovere di diligenza: i risultati di indagini che saranno condotte dalla Commissione con il sostegno dell'ENISA sia per gli utilizzatori sia per le imprese.

Per valutare l'attuazione, la Commissione intende garantire che le valutazioni della conformità siano condotte in modo efficace. A tal fine sarà emessa una richiesta di normazione e ne verrà seguita l'attuazione. La Commissione verificherà inoltre la capacità degli organismi notificati e, se del caso, degli organismi di certificazione.

Per quanto riguarda l'applicazione, mediante le relazioni degli Stati membri la Commissione verificherà che le iniziative nazionali non riguardino aspetti oggetto del regolamento.

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa

Il regolamento dovrebbe essere pienamente applicabile 24 mesi dopo la sua entrata in vigore. Tuttavia gli elementi della struttura di governance dovrebbero essere posti in essere prima di tale data. In particolare gli Stati membri devono aver nominato le autorità già esistenti e/o istituito nuove autorità con la funzione di svolgere i compiti previsti dalla normativa.

1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.

La forte natura transfrontaliera della cibersicurezza e i crescenti incidenti, con effetti di ricaduta a livello transfrontaliero e trasversalmente ai settori e ai prodotti, fanno sì che gli obiettivi non possano essere raggiunti efficacemente dai soli Stati membri. Data la natura globale dei mercati dei prodotti con elementi digitali, sul rispettivo territorio gli Stati membri si trovano ad affrontare gli stessi rischi per lo stesso

prodotto con elementi digitali. Il formarsi di un quadro frammentario di norme nazionali potenzialmente divergenti rischia inoltre di ostacolare la creazione di un mercato unico aperto e competitivo per i prodotti con elementi digitali. È quindi necessaria un'azione comune a livello dell'UE per aumentare il grado di fiducia degli utilizzatori e l'attrattiva dei prodotti con elementi digitali dell'UE. Tale azione avrebbe anche benefici per il mercato interno, garantendo la certezza del diritto e creando condizioni di parità per i venditori di prodotti con elementi digitali.

1.5.3. Insegnamenti tratti da esperienze analoghe

La legge sulla ciberresilienza è il primo regolamento del suo genere, che introduce requisiti di cibersicurezza per l'immissione sul mercato di prodotti con elementi digitali. Essa si basa tuttavia sull'impostazione del nuovo quadro normativo e sugli insegnamenti tratti dal processo di attuazione della normativa di armonizzazione dell'Unione vigente per una serie di prodotti, in particolare per quanto riguarda la preparazione all'attuazione, compresi aspetti quali la preparazione di norme armonizzate.

1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti

Il regolamento sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali definisce nuovi requisiti di cibersicurezza per tutti i prodotti con elementi digitali immessi sul mercato dell'UE, andando oltre i requisiti previsti dalla normativa vigente. Al contempo la proposta si basa sull'impostazione esistente della legislazione del nuovo quadro normativo. Pertanto si baserebbe sulle strutture e sulle procedure vigenti del nuovo quadro normativo, come la cooperazione degli organismi notificati e la vigilanza del mercato, i moduli di valutazione della conformità e lo sviluppo di norme armonizzate. La nuova proposta si fonderebbe inoltre su alcune strutture sviluppate in base ad altre normative in materia di cibersicurezza, come la direttiva 2016/1148 (direttiva NIS), la [direttiva XXX/XXXX (NIS2)] o il regolamento 2019/881 (regolamento sulla cibersicurezza).

1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione

La gestione dei settori d'intervento assegnati all'ENISA rientra nel suo mandato e nei suoi compiti generali. Tali settori d'intervento potrebbero richiedere profili specifici o nuovi incarichi, che tuttavia non sarebbero di grande rilievo e potrebbero essere assorbiti dalle risorse esistenti dell'ENISA e coperti mediante la riallocazione o il collegamento di vari incarichi. Ad esempio uno dei principali settori d'intervento assegnati all'ENISA riguarda la raccolta e il trattamento delle notifiche dei fabbricanti relative alle vulnerabilità sfruttate dei prodotti. Già nel quadro della [direttiva XXX/XXXX (NIS2)] l'ENISA è stata incaricata di istituire una banca dati europea delle vulnerabilità in cui le vulnerabilità pubblicamente note possano essere divulgate e registrate, su base volontaria, per consentire agli utilizzatori di adottare misure di attenuazione adeguate. Le risorse stanziate a tale scopo potrebbero essere utilizzate anche per i nuovi incarichi sopra citati relativi alle notifiche di vulnerabilità dei prodotti. In questo modo si potrebbe garantire un uso efficace delle risorse esistenti e si creerebbero inoltre le sinergie necessarie tra tali incarichi, che potrebbero orientare meglio le analisi dell'ENISA sulle minacce e sui rischi di cibersicurezza.

1.6. Durata e incidenza finanziaria della proposta/iniziativa

☐ **durata limitata**

– ☐ in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

– ☐ incidenza finanziaria dal AAAA al AAAA per gli stanziamenti di impegno e dal AAAA al AAAA per gli stanziamenti di pagamento

× **durata illimitata**

– attuazione con un periodo di avviamento a partire dal 2025

– e successivo funzionamento a pieno ritmo.

1.7. Modalità di gestione previste[40]

☐ **Gestione diretta** a opera della Commissione

– × a opera dei suoi servizi, compreso il suo personale presso le delegazioni dell'Unione

– ☐ a opera delle agenzie esecutive

☐ **Gestione concorrente** con gli Stati membri

☐ **Gestione indiretta** affidando compiti di esecuzione del bilancio:

– ☐ a paesi terzi o organismi da questi designati;

– ☐ a organizzazioni internazionali e loro agenzie (specificare);

– ☐ alla BEI e al Fondo europeo per gli investimenti;

– ☐ agli organismi di cui agli articoli 70 e 71 del regolamento finanziario;

– ☐ a organismi di diritto pubblico;

– ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui sono dotati di sufficienti garanzie finanziarie;

– ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che sono dotati di sufficienti garanzie finanziarie;

– ☐ alle persone incaricate di attuare azioni specifiche della PESC a norma del titolo V TUE e indicate nel pertinente atto di base.

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

Osservazioni

Il presente regolamento assegna all'ENISA talune funzioni, in linea con il mandato esistente e in particolare con l'articolo 3, paragrafo 2, del regolamento 2019/881, che prevede che l'ENISA svolga i compiti che le sono attribuiti dagli atti giuridici dell'Unione che stabiliscono le misure per il ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla cibersicurezza. In particolare l'ENISA ha il compito di ricevere le notifiche dei fabbricanti relative alle vulnerabilità attivamente sfruttate contenute nei prodotti con elementi digitali, nonché agli incidenti che hanno un impatto sulla sicurezza di tali prodotti. L'ENISA dovrebbe inoltre trasmettere tali notifiche ai pertinenti CSIRT o ai

[40] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: https://myintracomm.ec.europa.eu/budgweb/IT/man/budgmanag/Pages/budgmanag.aspx.

pertinenti punti di contatto unici degli Stati membri designati conformemente all'articolo [articolo X] della direttiva [direttiva XXX/XXXX (NIS2)] e informare le autorità di vigilanza del mercato. Sulla base delle informazioni raccolte, l'ENISA dovrebbe preparare una relazione tecnica biennale sulle tendenze emergenti relative ai rischi di cibersicurezza nei prodotti con elementi digitali e presentarla al gruppo di cooperazione NIS. Inoltre, considerando le sue competenze, le informazioni raccolte e le analisi delle minacce, l'ENISA può sostenere il processo di attuazione del presente regolamento proponendo attività congiunte che saranno svolte dalle autorità nazionali di vigilanza del mercato sulla base di indicazioni o informazioni riguardanti la potenziale non conformità al presente regolamento di prodotti con elementi digitali in diversi Stati membri o individuare categorie di prodotti per le quali possono essere organizzate azioni di controllo coordinate e simultanee. La Commissione può chiedere all'ENISA di effettuare valutazioni per prodotti specifici in circostanze eccezionali in relazione a prodotti con elementi digitali che presentano un rischio di cibersicurezza significativo e qualora sia necessario un intervento immediato per preservare il buon funzionamento del mercato interno.

Tutti questi incarichi sono stimati a circa 4,5 ETP dalle risorse esistenti dell'ENISA, basandosi già sulle competenze e sui lavori preparatori attualmente svolti dall'ENISA, tra l'altro a sostegno dell'imminente attuazione della [direttiva XXX/XXXX (NIS2)], per la quale le risorse dell'ENISA sono state integrate.

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

Entro 36 mesi dalla data di applicazione del presente regolamento e successivamente ogni quattro anni la Commissione trasmette al Parlamento europeo e al Consiglio una relazione sulla valutazione e sul riesame del regolamento. Le relazioni sono pubblicate.

2.2. Sistema di gestione e di controllo

2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti

Il presente regolamento stabilisce una nuova politica in materia di requisiti armonizzati di cibersicurezza per i prodotti con elementi digitali immessi sul mercato interno durante l'intero ciclo di vita. L'atto giuridico sarà seguito da richieste da parte della Commissione agli organismi europei di normazione relative allo sviluppo di norme.

Al fine di far fronte a tali nuovi compiti, è necessario fornire risorse adeguate ai servizi della Commissione. Si stima che l'applicazione del nuovo regolamento richieda 7 ETP (di cui uno END) per occuparsi dei compiti seguenti:

- preparazione della richiesta di normazione e/o delle specifiche comuni tramite atti di esecuzione in assenza di un valido processo di normazione;
- preparazione di un atto delegato [entro 12 mesi dall'entrata in vigore del regolamento] che specifichi le definizioni dei prodotti con elementi digitali critici;
- eventuale preparazione di atti delegati per l'aggiornamento dell'elenco dei prodotti critici di classe I e II; specificare se è necessaria una limitazione o un'esclusione per i prodotti con elementi digitali disciplinati da altre norme dell'Unione che stabiliscono requisiti che conseguono lo stesso livello di protezione del presente regolamento; imporre la certificazione di determinati prodotti con elementi digitali altamente critici sulla base dei criteri stabiliti nel presente regolamento; specificare il contenuto minimo della dichiarazione di conformità UE e integrare gli elementi da includere nella documentazione tecnica;
- eventuale preparazione di atti di esecuzione relativi al formato o agli elementi degli obblighi di segnalazione, alla distinta base del software, alle specifiche comuni o all'apposizione della marcatura CE;
- eventuale preparazione di un intervento immediato per imporre misure correttive o restrittive in circostanze eccezionali per preservare il buon funzionamento del mercato interno, compresa la preparazione di un atto di esecuzione;
- organizzazione e coordinamento delle notifiche trasmesse dagli Stati membri relative agli organismi notificati e coordinamento di questi ultimi;

– sostegno al coordinamento delle autorità di vigilanza del mercato degli Stati membri.

2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli

Per garantire che gli organismi notificati e le autorità di vigilanza del mercato si scambino informazioni e cooperino in modo ottimale, la Commissione è responsabile del loro coordinamento. Per le competenze tecniche e di mercato sarà creato un gruppo di esperti.

2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)

2.3. Quanto alle spese per riunioni, dato il basso valore per transazione (ad esempio rimborso delle spese di viaggio per un delegato per una riunione), le procedure di controllo abituali paiono sufficienti. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste, ad esempio strategia antifrode.

Le vigenti misure di prevenzione delle frodi applicabili alla Commissione si applicheranno agli stanziamenti supplementari necessari per il presente regolamento.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

Schema

- Nuove linee di bilancio di cui è chiesta la creazione

N/P

3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti

3.2.1. Sintesi dell'incidenza prevista sugli stanziamenti operativi

– ☑ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi

– ☐ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	Numero	

DG: <…….>			Anno **N**[41]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
• Stanziamenti operativi										
Linea di bilancio[42]	Impegni	(1a)								
	Pagamenti	(2a)								
Linea di bilancio	Impegni	(1b)								
	Pagamenti	(2b)								
Stanziamenti amministrativi finanziati dalla dotazione di programmi specifici[43]										
Linea di bilancio		(3)								
TOTALE stanziamenti per la DG <….>	Impegni	=1a+1b +3								
	Pagamenti	=2a+2b								

41 L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es. 2021) e così per gli anni a seguire.

42 Secondo la nomenclatura di bilancio ufficiale.

43 Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

		+3								

• TOTALE stanziamenti operativi	Impegni	(4)								
	Pagamenti	(5)								
• TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici		(6)								
TOTALE stanziamenti per la RUBRICA <….> del quadro finanziario pluriennale	Impegni	=4+ 6								
	Pagamenti	=5+ 6								

Se la proposta/iniziativa incide su più rubriche operative, ricopiare nella sezione sotto:

• TOTALE stanziamenti operativi (tutte le rubriche operative)	Impegni	(4)								
	Pagamenti	(5)								
TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici (tutte le rubriche operative)		(6)								
TOTALE stanziamenti per le RUBRICHE da 1 a 6 del quadro finanziario pluriennale (importo di riferimento)	Impegni	=4+ 6								
	Pagamenti	=5+ 6								

Rubrica del quadro finanziario pluriennale	7	"Spese amministrative"

Sezione da compilare utilizzando i "dati di bilancio di natura amministrativa" che saranno introdotti nell'allegato della scheda finanziaria legislativa (allegato V delle norme interne), caricato su DECIDE a fini di consultazione interservizi.

Mio EUR (al terzo decimale)

		Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
DG: CNECT						
• Risorse umane		1,030	1,030	1,030	1,030	**4,120**
• Altre spese amministrative		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
TOTALE DG CNECT	Stanziamenti	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

TOTALE stanziamenti per la RUBRICA 7 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

Mio EUR (al terzo decimale)

		Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	**TOTALE**
TOTALE stanziamenti per le RUBRICHE da 1 a 7 del quadro finanziario pluriennale	Impegni	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Pagamenti	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Risultati previsti finanziati con gli stanziamenti operativi

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati ⇩			Anno **N**		Anno **N+1**		Anno **N+2**		Anno **N+3**		Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)						**TOTALE**	
	RISULTATI																	
	Tipo[44]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[45]…																		
- Risultato																		
- Risultato																		
- Risultato																		
Totale parziale obiettivo specifico 1																		
OBIETTIVO SPECIFICO 2																		
- Risultato																		
Totale parziale obiettivo specifico 2																		
TOTALE																		

[44] I risultati sono i prodotti e i servizi da fornire (ad es. numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

[45] Come descritto nella sezione 1.4.2. "Obiettivi specifici..."

3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi

– ☑ La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**	
RUBRICA 7 del quadro finanziario pluriennale					
Risorse umane	1,030	1,030	1,030	1,030	**4,120**
Altre spese amministrative	0,222	0,222	0,222	0,222	**0,888**
Totale parziale RUBRICA 7 del quadro finanziario pluriennale	1,252	1,252	1,252	1,252	**5,008**

Esclusa la RUBRICA 7[46] del quadro finanziario pluriennale					
Risorse umane					
Altre spese amministrative					
Totale parziale esclusa la RUBRICA 7 del quadro finanziario pluriennale					

TOTALE	1,252	1,252	1,252	1,252	**5,008**

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese amministrative è coperto dagli stanziamenti della DG già assegnati alla gestione dell'azione e/o riassegnati all'interno della stessa DG, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

[46] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.3.1. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– ☑ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in equivalenti a tempo pieno

		Anno **2024**	Anno **2025**	Anno **2026**	Anno **2027**
20 01 02 01 (sede e uffici di rappresentanza della Commissione)		6	6	6	6
20 01 02 03 (delegazioni)					
01 01 01 01 (ricerca indiretta)					
01 01 01 11 (ricerca diretta)					
Altre linee di bilancio (specificare)					
• Personale esterno (in equivalenti a tempo pieno: ETP)[47]					
20 02 01 (AC, END, INT della dotazione globale)		1	1	1	1
20 02 03 (AC, AL, END, INT e JPD nelle delegazioni)					
XX 01 xx **yy zz** [48]	- in sede				
	- nelle delegazioni				
01 01 01 02 (AC, END, INT - ricerca indiretta)					
01 01 01 12 (AC, END, INT - ricerca diretta)					
Altre linee di bilancio (specificare)					
TOTALE		**7**	**7**	**7**	**7**

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei 6 ETP x 157 000 EUR/anno = 942 000 EUR	Come descritto nella sezione 2.2.1: – preparazione della richiesta di normazione e/o delle specifiche comuni tramite atti di esecuzione in assenza di un valido processo di normazione; – preparazione di un atto delegato [entro 12 mesi dall'entrata in vigore del regolamento] che specifichi le definizioni dei prodotti con elementi digitali critici; – eventuale preparazione di atti delegati per l'aggiornamento dell'elenco dei prodotti critici di classe I e II; specificare se è necessaria una limitazione o un'esclusione per i prodotti con elementi digitali disciplinati da altre norme dell'Unione che stabiliscono requisiti che conseguono lo stesso livello di protezione del presente regolamento; imporre la certificazione di determinati prodotti con elementi digitali altamente critici sulla base dei criteri stabiliti nel presente regolamento; specificare il contenuto minimo della dichiarazione di conformità UE e integrare gli elementi da includere nella documentazione tecnica; – eventuale preparazione di atti di esecuzione relativi al formato o agli

[47] AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JPD = giovane professionista in delegazione.

[48] Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

	elementi degli obblighi di segnalazione, alla distinta base del software, alle specifiche comuni o all'apposizione della marcatura CE; – eventuale preparazione di un intervento immediato per imporre misure correttive o restrittive in circostanze eccezionali per preservare il buon funzionamento del mercato interno, compresa la preparazione di un atto di esecuzione; – organizzazione e coordinamento delle notifiche trasmesse dagli Stati membri relative agli organismi notificati e coordinamento di questi ultimi; – sostegno al coordinamento delle autorità di vigilanza del mercato degli Stati membri.
Personale esterno 1 END x 88 000 EUR/anno	Come descritto nella sezione 2.2.1: – preparazione della richiesta di normazione e/o delle specifiche comuni tramite atti di esecuzione in assenza di un valido processo di normazione; – preparazione di un atto delegato [entro 12 mesi dall'entrata in vigore del regolamento] che specifichi le definizioni dei prodotti con elementi digitali critici; – eventuale preparazione di atti delegati per l'aggiornamento dell'elenco dei prodotti critici di classe I e II; specificare se è necessaria una limitazione o un'esclusione per i prodotti con elementi digitali disciplinati da altre norme dell'Unione che stabiliscono requisiti che conseguono lo stesso livello di protezione del presente regolamento; imporre la certificazione di determinati prodotti con elementi digitali altamente critici sulla base dei criteri stabiliti nel presente regolamento; specificare il contenuto minimo della dichiarazione di conformità UE e integrare gli elementi da includere nella documentazione tecnica; – eventuale preparazione di atti di esecuzione relativi al formato o agli elementi degli obblighi di segnalazione, alla distinta base del software, alle specifiche comuni o all'apposizione della marcatura CE; – eventuale preparazione di un intervento immediato per imporre misure correttive o restrittive in circostanze eccezionali per preservare il buon funzionamento del mercato interno, compresa la preparazione di un atto di esecuzione; – organizzazione e coordinamento delle notifiche trasmesse dagli Stati membri relative agli organismi notificati e coordinamento di questi ultimi; – sostegno al coordinamento delle autorità di vigilanza del mercato degli Stati membri.

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

La proposta/iniziativa:

– x può essere interamente finanziata mediante riassegnazione all'interno della pertinente rubrica del quadro finanziario pluriennale (QFP).

Non è necessaria alcuna riprogrammazione.

– ☐ comporta l'uso del margine non assegnato della pertinente rubrica del QFP e/o l'uso degli strumenti speciali definiti nel regolamento QFP.

-

– ☐ comporta una revisione del QFP.

-

3.2.5. Partecipazione di terzi al finanziamento

La proposta/iniziativa:

– x non prevede cofinanziamenti da terzi

– ☐ prevede il cofinanziamento da terzi indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

	Anno **N**[49]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			Totale
Specificare l'organismo di cofinanziamento								
TOTALE stanziamenti cofinanziati								

[49] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es. 2021) e così per gli anni a seguire.

3.3. Incidenza prevista sulle entrate

– ☐ La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

  – ☐ sulle risorse proprie

  – ☐ su altre entrate

  – indicare se le entrate sono destinate a linee di spesa specifiche ☐

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanziamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa[50]						
		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
Articolo …….								

Per quanto riguarda le entrate con destinazione specifica, precisare la o le linee di spesa interessate.

Altre osservazioni (ad es. formula/metodo per calcolare l'incidenza sulle entrate o altre informazioni).

[50] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20 % per spese di riscossione.