Parlamento europeo
2019-2024

Documento di seduta

A9-0253/2023

26.7.2023

***I
RELAZIONE

sulla 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
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Commissione per l'industria, la ricerca e l'energia

Relatore: Nicola Danti

Relatore per parere della commissione associata a norma dell'articolo 57 del regolamento:
Morten Løkkegaard, commissione per il mercato interno e la protezione dei consumatori

Significato dei simboli utilizzati

*	Procedura di consultazione
***	Procedura di approvazione
***I	Procedura legislativa ordinaria (prima lettura)
***II	Procedura legislativa ordinaria (seconda lettura)
***III	Procedura legislativa ordinaria (terza lettura)

(La procedura indicata dipende dalla base giuridica proposta nel progetto di atto)

Emendamenti a un progetto di atto

Emendamenti del Parlamento presentati su due colonne

Le soppressioni sono evidenziate in ***corsivo grassetto*** nella colonna di sinistra. Le sostituzioni sono evidenziate in ***corsivo grassetto*** nelle due colonne. Il testo nuovo è evidenziato in ***corsivo grassetto*** nella colonna di destra.

La prima e la seconda riga del blocco d'informazione di ogni emendamento identificano la parte di testo interessata del progetto di atto in esame. Se un emendamento verte su un atto esistente che il progetto di atto intende modificare, il blocco d'informazione comprende anche una terza e una quarta riga che identificano rispettivamente l'atto esistente e la disposizione interessata di quest'ultimo.

Emendamenti del Parlamento presentati in forma di testo consolidato

Le parti di testo nuove sono evidenziate in ***corsivo grassetto***. Le parti di testo soppresse sono indicate con il simbolo ▌ o sono barrate. Le sostituzioni sono segnalate evidenziando in ***corsivo grassetto*** il testo nuovo ed eliminando o barrando il testo sostituito.
A titolo di eccezione, le modifiche di carattere strettamente tecnico apportate dai servizi in vista dell'elaborazione del testo finale non sono evidenziate.

INDICE

Pagina

PROGETTO DI RISOLUZIONE LEGISLATIVA DEL PARLAMENTO EUROPEO

sulla 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
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

(Procedura legislativa ordinaria: prima lettura)

Il Parlamento europeo,

– vista la proposta della Commissione al Parlamento europeo e al Consiglio (COM(2022)0454),

– visti l'articolo 294, paragrafo 2, e l'articolo 114 del trattato sul funzionamento dell'Unione europea, a norma dei quali la proposta gli è stata presentata dalla Commissione (C9-0308/2022),

– visto l'articolo 294, paragrafo 3, del trattato sul funzionamento dell'Unione europea,

– visto il parere del Comitato economico e sociale europeo del 14 dicembre 2022[1],

– visto l'articolo 59 del suo regolamento,

– visto il parere della commissione per il mercato interno e la protezione dei consumatori,

– vista la relazione della commissione per l'industria, la ricerca e l'energia (A9-0253/2023),

1. adotta la posizione in prima lettura figurante in appresso;

2. chiede alla Commissione di modificare la scheda finanziaria che accompagna la proposta aumentando la tabella dell'organico dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) di 9,0 posti supplementari a tempo pieno e fornendo i corrispondenti stanziamenti supplementari al fine di garantire che gli obblighi dell'ENISA a norma del presente regolamento possano essere soddisfatti e di non compromettere gli obblighi esistenti dell'Agenzia previsti da altre normative dell'Unione;

3. chiede alla Commissione di presentargli nuovamente la proposta qualora la sostituisca, la modifichi sostanzialmente o intenda modificarla sostanzialmente;

4. incarica la sua Presidente di trasmettere la posizione del Parlamento al Consiglio e alla Commissione nonché ai parlamenti nazionali.

[1] GU C 100 del 16.3.2023, pag. 101;

Emendamento 1

EMENDAMENTI DEL PARLAMENTO EUROPEO*

alla proposta della Commissione

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 ***e la direttiva 2020/1828/CE (legge sulla ciberresilienza)***

(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[2],

visto il parere del Comitato delle regioni[3],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) ***La cibersicurezza è una delle sfide principali per l'Unione e il numero e la varietà dei dispositivi connessi aumenteranno esponenzialmente nei prossimi anni. Gli attacchi informatici costituiscono una questione di interesse pubblico dal momento che hanno un impatto determinante non solo sull'economia dell'Unione, ma anche sulla democrazia e sulla sicurezza e salute dei consumatori.*** Occorre ***pertanto***

* Emendamenti: il testo nuovo o modificato è evidenziato in grassetto corsivo e le soppressioni sono segnalate con il simbolo ▌.

2 GU C ***100 del 16.3.2023***, pag. ***101.***

3 GU C […] del […], pag. […].

rafforzare l'approccio dell'Unione alla cibersicurezza, occuparsi della ciberresilienza a livello dell'Unione nonché 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***, ad esempio migliorando la trasparenza per quanto riguarda il periodo di assistenza dei prodotti immessi sul mercato***.

(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 cibersicurezza, tra cui il regolamento (UE) 2019/881 del Parlamento e del Consiglio[4] ***e la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[5]***, non contempla direttamente requisiti obbligatori per la sicurezza dei prodotti con elementi digitali.

---

[4] 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).

[5] ***Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80).***

(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 ***e alle organizzazioni*** 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***, al fine di garantire un quadro normativo armonizzato e chiaro per le imprese, in particolare le microimprese e le piccole e medie imprese.*** 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 ***e proporzionalità per le micro, piccole e medie imprese***, creando condizioni più agevoli per gli operatori ***economici*** che intendono entrare nel mercato dell'Unione.

(4 bis) Essendo di carattere orizzontale, il presente regolamento avrà un impatto su segmenti molto diversi dell'economia dell'Unione. È pertanto importante che si tenga conto delle specificità di ciascun settore e che i requisiti di cibersicurezza di cui al presente regolamento siano proporzionati ai rischi. La Commissione dovrebbe pertanto emanare orientamenti che illustrino in modo chiaro e dettagliato le modalità di applicazione del presente regolamento. Gli orientamenti dovrebbero comprendere, tra l'altro, una spiegazione dettagliata dell'ambito di applicazione, in particolare per quanto riguarda la nozione di trattamento a distanza dei dati e le implicazioni per gli sviluppatori di software liberi e open source, i criteri utilizzati per determinare le modalità di classificazione dei prodotti critici con elementi digitali e l'interazione tra il presente regolamento e altre normative dell'Unione.

(4 ter) Un'impresa che opera online può offrire una varietà di servizi diversi. A seconda della natura dei servizi forniti, lo stesso soggetto può rientrare in diverse categorie

di operatori economici. Se un soggetto fornisce servizi di intermediazione online per un prodotto con elementi digitali ed è un fornitore di un mercato online quale definito all'articolo 3, paragrafo 14, del regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio[6], tale soggetto non si qualifica come operatore economico ai sensi del presente regolamento. Qualora lo stesso soggetto sia un fornitore di un mercato online e agisca in qualità di operatore economico quale definito nel presente regolamento per la vendita di prodotti con elementi digitali, esso dovrebbe essere soggetto all'ambito di applicazione del presente regolamento per quanto riguarda tali prodotti. Le disposizioni del regolamento (UE) 2023/988 sono pienamente applicabili al presente regolamento. Dato il ruolo di primo piano svolto dai mercati online nel consentire il commercio elettronico, essi dovrebbero adoperarsi per cooperare con le autorità di vigilanza del mercato degli Stati membri al fine di garantire che i prodotti acquistati attraverso i mercati online siano conformi ai requisiti di cibersicurezza di cui al presente regolamento.

(5) A livello dell'Unione diversi documenti programmatici e politici, come la strategia dell'UE in materia di cibersicurezza per il decennio digitale[7], le conclusioni del Consiglio del 2 dicembre 2020 e del 23 maggio 2022 o la risoluzione del Parlamento europeo del 10 giugno 2021[8], 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[9], i cittadini hanno chiesto "un ruolo più incisivo dell'UE nella lotta contro le minacce alla cibersicurezza". ***Affinché l'Unione possa svolgere un ruolo di primo piano a livello internazionale***

---

6 ***Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio, del 10 maggio 2023, relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio (GU L 135 del 23.5.2023, pag. 1).***

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

8 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_IT.html.

9 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.

nel settore della cibersicurezza, è importante istituire un quadro normativo generale ambizioso.

(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 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. ***Tali requisiti garantiranno inoltre che la cibersicurezza sia presa in considerazione in tutte le catene di approvvigionamento, rendendo più sicuri i prodotti finali con elementi digitali. Ciò rappresenterà a sua volta un vantaggio competitivo per i fabbricanti stabiliti o rappresentati nell'Unione, che saranno in grado di pubblicizzare la cibersicurezza dei loro prodotti.***

(9) Il presente regolamento garantisce un livello elevato di cibersicurezza dei prodotti con elementi digitali ***e delle loro soluzioni integrate di elaborazione dati da remoto***. ***Tali*** soluzioni di elaborazione dati da remoto relative a un prodotto con elementi digitali ***sono definite*** come una qualsiasi elaborazione dati a distanza per la quale il software è progettato e sviluppato dal fabbricante del prodotto in questione ***o per suo conto*** ▌ e la cui assenza impedirebbe a tale prodotto con elementi digitali di svolgere una delle sue funzioni. ***Ad esempio, le funzionalità abilitate al cloud fornite dal fabbricante di dispositivi domestici intelligenti che consentono agli utenti di controllare il dispositivo a distanza dovrebbero rientrare nell'ambito di applicazione del presente regolamento. D'altro canto, i siti web non indissolubilmente collegati a un prodotto con elementi digitali o servizi cloud che esulano dalla responsabilità del fabbricante non dovrebbero essere considerati soluzioni di elaborazione dati da remoto ai sensi del presente regolamento.*** La direttiva ***(UE) 2022/2555*** 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. ***Sebbene la direttiva (UE) 2022/2555*** si ***applichi*** ai servizi di cloud computing e ai modelli di servizi cloud ***e il presente regolamento non si applichi a servizi come il servizio a livello di software (Software-as-a-Service – SaaS), il servizio a livello di piattaforma (Platform-as-a-Service – PaaS) o il servizio a livello di infrastruttura (Infrastructure-as-a-Service – IaaS), essi possono rientrare nell'ambito di applicazione del presente regolamento nella misura in cui soddisfano la definizione di soluzioni di elaborazione dati da remoto***. ▌

(10 bis) Il software e i dati che sono condivisi apertamente e ai quali gli utilizzatori possono accedere liberamente e che essi possono liberamente utilizzare, modificare e ridistribuire anche in versioni modificate, possono contribuire alla ricerca e all'innovazione nel mercato. Dalle ricerche condotte dalla Commissione europea[10] emerge anche che i software liberi e open source possono contribuire al PIL dell'Unione per un valore compreso tra i 65 e i 95 miliardi di EUR e offrire notevoli opportunità di crescita per l'economia dell'Unione. Gli utilizzatori possono eseguire,

[10] *The impact of open source software and hardware on technology independence, competitiveness and innovation in the EU economy* (L'impatto dei software e degli hardware open source sull'indipendenza tecnologica, sulla competitività e sull'innovazione nell'economia dell'UE), Commissione europea, 6 settembre 2021, https://ec.europa.eu/newsroom/dae/redirection/document/79021.

copiare, distribuire, studiare, modificare e migliorare i software e i dati, compresi i modelli, mediante licenze libere e open source. Per promuovere lo sviluppo e l'utilizzo di software liberi e open source, in particolare da parte delle microimprese e delle piccole e medie imprese, comprese le start-up, e delle organizzazioni senza scopo di lucro, della ricerca accademica e degli individui, il presente regolamento dovrebbe applicarsi ai prodotti software liberi e open source in casi specifici, per tenere conto del fatto che esistono diversi modelli di sviluppo di software che sono distribuiti e sviluppati con licenze pubbliche.

(10) ▌Il presente regolamento dovrebbe disciplinare ***solo*** il software libero e open source ▌***messo a disposizione sul mercato nel corso di*** un'attività commerciale. ▌ ***La valutazione che determina se un prodotto libero e open source sia stato messo a disposizione nell'ambito di un'attività commerciale dovrebbe essere effettuata prodotto per prodotto, considerando sia il modello di sviluppo sia la fase di fornitura del prodotto libero e open source con elementi digitali.***

(10 bis) Ad esempio, un modello di sviluppo completamente decentrato, in cui nessun singolo soggetto commerciale esercita il controllo su ciò che è accettato nella base di codice del progetto, dovrebbe essere considerato come un'indicazione del fatto che il prodotto è stato sviluppato in un contesto non commerciale. D'altro canto, è opportuno considerare un'attività come commerciale quando un software libero e open source è sviluppato da una singola organizzazione o da una comunità asimmetrica, laddove una singola organizzazione genera entrate da un utilizzo correlato in rapporti commerciali. Analogamente, se i principali contributori ai progetti liberi e open source sono sviluppatori impiegati da soggetti commerciali e se tali sviluppatori o il datore di lavoro possono esercitare un controllo su quali modifiche vengono accettate nella base di codice, il progetto dovrebbe essere generalmente considerato di natura commerciale.

(10 ter) Per quanto riguarda la fase di fornitura, nel contesto del software ***libero e open source***, 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, ***quando ciò non è finalizzato esclusivamente a recuperare i costi effettivi,*** 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. ***L'atto di accettare donazioni senza fini di lucro non dovrebbe essere considerato costitutivo di un'attività commerciale, a meno che tali donazioni non siano effettuate da soggetti commerciali e siano di natura ricorrente.***

(10 quater) Gli sviluppatori che contribuiscono a titolo individuale a progetti liberi e open source non dovrebbero essere soggetti agli obblighi del presente regolamento.

(10 quinquies) Il solo fatto di ospitare software liberi e open source su archivi aperti non costituisce di per sé una messa a disposizione sul mercato di un prodotto con elementi digitali. Pertanto, la maggior parte dei gestori di pacchetti, delle piattaforme di code hosting e di collaborazione non dovrebbero essere considerati distributori ai sensi del presente regolamento.

(10 sexies) Al fine di garantire che i prodotti siano progettati, sviluppati e prodotti conformemente ai requisiti essenziali di cui all'allegato I, sezione 1, i fabbricanti dovrebbero esercitare la dovuta diligenza quando integrano componenti provenienti da terzi, anche nel caso di software liberi e open source che non sono stati messi a disposizione sul mercato. Il livello adeguato di dovuta diligenza dipende dalla natura e dal livello di rischio del componente e può comprendere una o più delle seguenti azioni: verificare se il componente reca già la marcatura CE, controllare la cronologia degli aggiornamenti di sicurezza, verificare se è esente da vulnerabilità registrate nella banca dati europea delle vulnerabilità o in altre banche dati pubbliche oppure effettuare ulteriori test di sicurezza. Qualora, nell'esercizio della dovuta diligenza, il fabbricante del prodotto individui una vulnerabilità in un componente, anche in un componente libero e open source, dovrebbe informare lo sviluppatore del componente, provvedere a eliminare la vulnerabilità e, se del caso, fornire allo sviluppatore la correzione di sicurezza applicata. Dopo aver immesso il prodotto sul mercato, il fabbricante dovrebbe avere la responsabilità di garantire che le vulnerabilità siano gestite durante tutto il periodo di assistenza, anche per i componenti liberi e open source integrati nel prodotto con elementi digitali.

(10 septies) La mancanza di competenze professionali in materia di cibersicurezza è una questione che è essenziale affrontare per assicurare un'applicazione efficace del presente regolamento. Occorre prestare particolare attenzione alla carenza di competenze dei fabbricanti, delle autorità di vigilanza del mercato e degli organismi

notificati. Pertanto, in linea con la comunicazione della Commissione dal titolo "Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE ('Accademia per le competenze in materia di cibersicurezza')", è opportuno adottare misure specifiche a livello di Unione e di Stati membri per valutare lo stato e l'evoluzione del mercato del lavoro nel settore della cibersicurezza e le sinergie per le offerte di istruzione e formazione nel campo della cibersicurezza, anche affrontando il divario di genere nel settore, con l'obiettivo di stabilire un approccio comune dell'Unione alla formazione in materia di cibersicurezza.

(11) Lo sviluppo di un'internet sicura è indispensabile per il funzionamento delle infrastrutture critiche e per la società nel suo complesso. La direttiva ***(UE) 2022/2555*** 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 ***(UE) 2022/2555*** 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[11] stabilisce norme relative ai dispositivi medici e il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio[12] stabilisce norme relative ai dispositivi medico-diagnostici in vitro. Entrambi i regolamenti si occupano di rischi di cibersicurezza e adottano

[11] 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).

[12] 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).

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[13]. I prodotti con elementi digitali a cui si applica uno dei due regolamenti non dovrebbero pertanto essere soggetti al presente regolamento.

(12 bis) I prodotti con elementi digitali sviluppati esclusivamente per scopi di sicurezza nazionale o militari o i prodotti specificamente progettati per trattare informazioni classificate non rientrano nell'ambito di applicazione del presente regolamento. Tuttavia, gli Stati membri sono incoraggiati a garantire per tali prodotti un livello di protezione uguale o superiore a quello dei prodotti che rientrano nell'ambito di applicazione del presente regolamento.

(13) Il regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio[14] 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

---

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

14 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*).

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 cibersicurezza[15] e prevedendo specifiche procedure di valutazione della conformità. Nel settore dell'aviazione, il regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio[16] 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

---

15 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].

16 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).

dovrebbero essere applicate tali limitazioni o esclusioni, il presente regolamento contiene disposizioni specifiche per chiarire il suo rapporto con tale normativa dell'Unione.

(14 bis) Al fine di garantire che i prodotti messi a disposizione sul mercato possano essere riparati in modo efficace e che la loro durabilità possa essere estesa, è opportuno prevedere un'esenzione per i pezzi di ricambio. Ciò dovrebbe valere sia per i pezzi di ricambio che hanno lo scopo di riparare prodotti preesistenti messi a disposizione prima della data di applicazione del presente regolamento sia per i pezzi di ricambio che sono già stati sottoposti a una procedura di valutazione della conformità ai sensi del presente regolamento e che sono forniti dallo stesso fabbricante.

(14 ter) Il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio[17] stabilisce una serie di requisiti per garantire la sicurezza delle reti e dei sistemi informativi a sostegno dei processi operativi dei soggetti finanziari. La Commissione dovrebbe monitorare l'attuazione del presente regolamento nel settore finanziario, al fine di garantirne la compatibilità e di evitare sovrapposizioni per i prodotti con elementi digitali che possono rientrare anche nell'ambito di applicazione del regolamento (UE) 2022/2554.

(14 quater) I veicoli agricoli e forestali che rientrano nell'ambito di applicazione del regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio[18] rientrano anche nell'ambito di applicazione del presente regolamento. Le future modifiche del regolamento (UE) n. 167/2013 dovrebbero evitare sovrapposizioni normative.

(15) Il regolamento delegato (UE) 2022/30 ***della Commissione***[19] 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

---

17 ***Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1).***

18 ***Regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio, del 5 febbraio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli agricoli e forestali (GU L 60 del 2.3.2013, pag. 1).***

19 ***Regolamento delegato (UE) 2022/30 della Commissione, del 29 ottobre 2021, che integra la direttiva 2014/53/UE del Parlamento europeo e del Consiglio per quanto riguarda l'applicazione dei requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere d), e) ed f), di tale direttiva (GU L 7 del 12.1.2022, pag. 6).***

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, ***quando*** la Commissione ▌ modifica il 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. ***I costruttori che si conformano al presente regolamento prima della sua data di applicazione dovrebbero essere considerati conformi anche al regolamento delegato (UE) 2022/30 della Commissione fino all'abrogazione di tale regolamento delegato da parte della Commissione.***

(16) La direttiva 85/374/CEE ***del Consiglio***[20] 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.

---

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

(17) Il presente regolamento dovrebbe lasciare impregiudicato il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[21], 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.

(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

[21] 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).

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.

(18 bis) Nell'acquistare prodotti con elementi digitali, gli Stati membri dovrebbero dare la priorità ai prodotti che hanno un elevato livello di cibersicurezza e un periodo di assistenza adeguato, al fine di migliorare la loro capacità di far fronte alle minacce informatiche, nonché di garantire l'uso efficiente delle risorse pubbliche. Inoltre, gli Stati membri dovrebbero garantire che i fabbricanti pongano rimedio, con urgenza, alle vulnerabilità che interessano i prodotti con elementi digitali oggetto di appalti pubblici, nei casi in cui tali prodotti presentano un profilo di rischio significativo.

(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 ***di rilievo*** che hanno un impatto sulla sicurezza di tali prodotti. ***Le vulnerabilità soggette a segnalazione obbligatoria riguardano i casi in cui un soggetto esegue un codice malevolo su un prodotto con elementi digitali al fine di generare una violazione della sicurezza, ad esempio sfruttando carenze nelle funzioni di identificazione e autenticazione. Le vulnerabilità scoperte senza intento doloso che hanno finalità di prova, indagine, correzione o divulgazione in buona fede nell'intento di promuovere la sicurezza del proprietario del sistema e dei suoi utenti non dovrebbero essere soggette a notifiche obbligatorie. Per incidente di rilievo che ha un impatto sulla sicurezza del prodotto con elementi digitali si intende un incidente di cibersicurezza che può incidere gravemente sui processi di sviluppo,***

produzione e manutenzione del fabbricante e che, a sua volta, può avere un impatto significativo sulla sicurezza dei suoi prodotti. Un tale incidente di rilievo potrebbe comprendere una situazione in cui l'autore di un attacco è riuscito a compromettere il canale di diffusione tramite il quale il fabbricante rilascia gli aggiornamenti di sicurezza agli utenti.

(19 bis) 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 ***(UE) 2022/2555*** e informare le autorità di vigilanza del mercato competenti in merito alla vulnerabilità notificata. ***L'ENISA dovrebbe garantire che tali notifiche siano ricevute, conservate e trasmesse attraverso canali sicuri e che siano predisposti protocolli chiari in merito alle persone autorizzate ad accedervi e alle modalità per la loro successiva trasmissione. L'ENISA dovrebbe altresì garantire la riservatezza di tali notifiche con particolare riguardo alle vulnerabilità per le quali non è ancora disponibile un aggiornamento di sicurezza.*** 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 ***(UE) 2022/2555***. 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 ***in modo visibile, leggibile e indelebile*** 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. ***Inoltre, in occasione di fiere, mostre e dimostrazioni o eventi analoghi, gli Stati membri non dovrebbero impedire la presentazione e l'uso di un prototipo di un prodotto con elementi digitali.***

(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***, in una versione non destinata alla produzione,*** 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 necessari per la sicurezza,*** gli aggiornamenti o le riparazioni del software***, come ad esempio piccoli aggiustamenti del codice sorgente che possono migliorare la sicurezza, non dovrebbero essere considerati modifiche sostanziali,*** 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. ***Ciò vale, in linea generale, per le nuove versioni del software che mirano a migliorare le prestazioni e a correggere le vulnerabilità. I piccoli aggiornamenti delle funzionalità, come ad esempio i miglioramenti visivi, l'aggiunta di nuove lingue all'interfaccia utente o di una nuova serie di pittogrammi,***

non dovrebbero, di norma, essere considerati modifiche sostanziali. 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***, come generalmente avviene per le revisioni del software***. ***La Commissione dovrebbe emanare orientamenti su come determinare la nozione di "modifica sostanziale".***

(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 ***(UE) 2022/2555***, o se si svolgono funzioni critiche o sensibili, ***che hanno un impatto sulla salute, la sicurezza o i diritti fondamentali***.

(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 ***ad alto rischio***, 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 I. 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 ***6*** 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. ***Al fine di garantire la chiarezza e la certezza del diritto, nonché la prevedibilità, affinché i portatori di interessi rispettino il presente regolamento, non dovrebbero essere apportate modifiche all'elenco di cui all'allegato III prima di due anni dopo l'entrata in vigore del presente regolamento e, successivamente, non prima di altri due anni. La Commissione dovrebbe stabilire una procedura in base alla quale tutti i portatori di interessi, compresi i fabbricanti e gli utilizzatori, in un processo collaborativo, possano esaminare un prodotto candidato a essere un prodotto critico al fine di valutare il rischio di sicurezza posto da potenziali problemi di cibersicurezza del prodotto, se e quanto la designazione del prodotto come critico***

possa ridurre tale rischio e i costi associati alla designazione del prodotto come critico, prima dell'adozione dei pertinenti atti delegati.

(27 bis) La Commissione dovrebbe istituire un gruppo di esperti sulla ciberresilienza (il "gruppo di esperti"), con una composizione ampia e diversificata. Il gruppo di esperti dovrebbe sostenere la Commissione al fine di garantire la corretta attuazione del presente regolamento, ad esempio fornendo consulenza alla Commissione in merito a eventuali modifiche dell'elenco dei prodotti critici di cui all'allegato III o analizzando in che modo le norme europee e internazionali possono consentire la conformità ai requisiti essenziali del presente regolamento. La Commissione dovrebbe consultare il gruppo di esperti ed effettuare consultazioni pubbliche in sede di elaborazione degli atti delegati e degli atti di esecuzione conformemente al presente regolamento, in modo da garantire che tutti i portatori di interessi possano fornire i contributi necessari.

(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 ***sempre*** connessi alla cibersicurezza***, ma possono essere la conseguenza di una violazione della sicurezza***. 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 ***(UE) 2023/988***. Pertanto, alla luce della natura mirata del presente regolamento, in deroga all'articolo 2, paragrafo 1, terzo comma, lettera b), del regolamento ***(UE) 2023/988***, il capo III, sezione 1, i capi V e VII e i capi da IX a XI del regolamento ***(UE) 2023/988*** 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 ***(UE) 2023/988***.

(29) I prodotti con elementi digitali classificati come sistemi di IA ad alto rischio conformemente all'articolo 6 del regolamento[22] [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

[22] Regolamento [regolamento sull'IA].

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 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 ***(UE) 2023/1230 del Parlamento europeo e del Consiglio***[23] 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 ***(UE) 2023/1230***, per quanto concerne la protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo nella misura

[23] Regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio, del 14 giugno 2023, relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio (GU L 165 del 29.6.2023, pag. 1).

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 ***per tutto il periodo di assistenza***, 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 ***rendere disponibili i loro prodotti senza vulnerabilità note sfruttabili che possano avere un impatto sulla sicurezza di tali prodotti, nonché per*** applicare in modo appropriato le norme armonizzate**,** le specifiche comuni ***o le norme internazionali*** adeguate.

(32 bis) I fabbricanti dovrebbero determinare il periodo di assistenza durante il quale garantiscono la gestione delle vulnerabilità, tenendo debitamente conto di vari

criteri, tra cui la durata prevista del prodotto, la natura del prodotto stesso, la disponibilità dell'ambiente operativo, le aspettative degli utilizzatori, in particolare dei consumatori, e, ove possibile, il periodo di assistenza di altri componenti principali integrati nel prodotto. I fabbricanti dovrebbero provvedere affinché il periodo di assistenza tenga adeguatamente conto della necessità di promuovere la cibersicurezza nel mercato dell'Unione e sia definito tenendo in debita considerazione il periodo durante il quale si prevede che un prodotto con elementi digitali sia disponibile sul mercato. Le autorità di vigilanza del mercato dovrebbero garantire proattivamente che i fabbricanti applichino tali criteri in modo adeguato. Le autorità di vigilanza del mercato e la Commissione dovrebbero raccogliere e analizzare i dati relativi ai periodi di assistenza stabiliti dai fabbricanti e alla durata prevista dei prodotti, in modo da garantire che il presente regolamento consegua il suo obiettivo di promuovere la cibersicurezza dei prodotti con elementi digitali. Tali analisi dovrebbero, tra l'altro, fungere da base per la valutazione da parte della Commissione del presente regolamento, una volta che questo diventi applicabile.

(32 ter) I fabbricanti dovrebbero garantire, ove tecnicamente fattibile, che nei prodotti con elementi digitali vi sia una chiara distinzione tra aggiornamenti di sicurezza e aggiornamenti delle funzionalità. Gli aggiornamenti di sicurezza, intesi a ridurre il livello di rischio o a porre rimedio a potenziali vulnerabilità, dovrebbero essere installati automaticamente, in particolare per i prodotti di consumo. Gli utilizzatori dovrebbero mantenere la possibilità di disattivare questa funzione, mediante un meccanismo chiaro e di facile utilizzo. Una volta che i fabbricanti non garantiscano più la gestione delle vulnerabilità dei prodotti con elementi digitali, essi dovrebbero informarne gli utilizzatori in modo chiaro e semplice, ad esempio mediante la visualizzazione di una notifica di facile utilizzo.

(32 quater) Se i fabbricanti stabiliscono un periodo di assistenza di durata inferiore a cinque anni e non offrono più la gestione delle vulnerabilità dei prodotti con elementi digitali, essi dovrebbero mettere il loro codice sorgente a disposizione delle imprese che desiderano fornire aggiornamenti di sicurezza e altri servizi analoghi. L'accesso dovrebbe essere reso disponibile solo nell'ambito di un accordo contrattuale che tuteli la proprietà del prodotto con elementi digitali e impedisca la diffusione del codice sorgente al grande pubblico, tranne nei casi in cui tale codice è già stato fornito sulla base di una licenza libera e aperta.

(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 ***dalla*** direttiva ***(UE) 2022/2555***▌, 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 ***(UE) 2022/2555***.

(34) Per garantire che i CSIRT nazionali e i punti di contatto unici designati conformemente ***alla*** direttiva ***(UE) 2022/2555*** 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 ▌divulgare le vulnerabilità risolte alla banca dati europea delle vulnerabilità istituita a norma della direttiva ***(UE) 2022/2555*** e gestita dall'ENISA▌ .***L'ENISA dovrebbe pubblicare le vulnerabilità notificate nella banca dati europea delle vulnerabilità e dovrebbe predisporre una procedura adeguata per quanto riguarda il processo di pubblicazione, al fine di dare ai fabbricanti il tempo di elaborare i necessari aggiornamenti di sicurezza e agli utilizzatori il tempo necessario per attuarli o per adottare altre misure correttive o di attenuazione. La banca dati europea delle vulnerabilità dovrebbe aiutare i fabbricanti a rilevare le vulnerabilità note sfruttabili riscontrate nei loro prodotti, al fine di garantire l'immissione sul mercato di prodotti sicuri.***

(34 bis) È necessario che l'Unione aumenti al massimo i benefici della sua apertura

economica, riducendo al minimo, nel contempo, i rischi derivanti dalla dipendenza economica da fornitori ad alto rischio, mediante un quadro strategico comune per la sicurezza economica dell'Unione[24]. La dipendenza da fornitori ad alto rischio di prodotti critici con elementi digitali comporta un rischio strategico che dovrebbe essere affrontato a livello dell'Unione, in particolare quando i prodotti critici con elementi digitali sono destinati a essere usati dai soggetti essenziali di cui alla direttiva (UE) 2022/2555. Simili rischi possono essere connessi a fattori come la giurisdizione applicabile al fabbricante, le caratteristiche della sua proprietà aziendale e i legami di controllo con il governo di un paese terzo in cui esso è stabilito, in particolare se un paese conduce uno spionaggio economico e se la sua legislazione impone l'accesso arbitrario a qualsiasi tipo di attività o dati aziendali, compresi i dati commercialmente sensibili, e può imporre obblighi a fini di intelligence senza un sistema democratico di bilanciamento dei poteri, un meccanismo di controllo, un giusto processo o il diritto di appellarsi a una magistratura indipendente. Le autorità di vigilanza del mercato e la Commissione dovrebbero formulare orientamenti e raccomandazioni mirate destinate agli operatori economici in modo da garantire l'adozione di opportune misure correttive qualora vi siano motivi sufficienti per ritenere che un prodotto con elementi digitali presenti un rischio di cibersicurezza significativo alla luce di tali fattori di rischio non tecnici.

(35) I fabbricanti dovrebbero anche segnalare all'ENISA qualsiasi incidente ***significativo*** che abbia un impatto sulla sicurezza del prodotto con elementi digitali. Fatti salvi gli obblighi di segnalazione degli incidenti previsti dalla direttiva ***(UE) 2022/2555*** 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 ***(UE) 2022/2555*** 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 ***significativi*** 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

---

24 ***Vedasi la comunicazione congiunta al Parlamento europeo, al Consiglio europeo e al Consiglio sulla "Strategia europea per la sicurezza economica" (JOIN(2023)0020).***

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.

(35 bis) I fabbricanti e gli altri soggetti e attori dovrebbero inoltre poter segnalare all'ENISA, su base volontaria, altri incidenti di cibersicurezza, minacce informatiche, quasi incidenti e qualsiasi altra vulnerabilità.

(35 ter) L'ENISA dovrebbe istituire un meccanismo di segnalazione digitale sicuro che, al fine di semplificare la segnalazione per i fabbricanti, dovrebbe fungere da punto di accesso unico per gli obblighi di segnalazione istituiti dal presente regolamento. I fabbricanti di prodotti con elementi digitali si trovano spesso in una situazione in cui un particolare incidente, in ragione delle sue caratteristiche, deve essere segnalato a varie autorità in conseguenza degli obblighi di notifica previsti da vari strumenti giuridici. Lo stesso meccanismo potrebbe, ove possibile, consentire la comunicazione a norma di altri atti legislativi dell'Unione, come il regolamento (UE) 2016/679, la direttiva (UE) 2022/2555 e la direttiva 2002/58/CE del Parlamento europeo e del Consiglio[25]. Il meccanismo può essere altresì utilizzato per le notifiche volontarie dei fabbricanti e di altri soggetti e attori. L'ENISA dovrebbe provvedere affinché essi dispongano di procedure per trattare le informazioni classificate in modo sicuro e riservato.

(35 quater) In alcuni Stati membri i soggetti e le persone fisiche che effettuano ricerche sulle vulnerabilità possono essere esposti alla responsabilità penale e civile. La Commissione dovrebbe formulare linee guida per quanto riguarda la non perseguibilità dei ricercatori in materia di sicurezza delle informazioni e l'esenzione dalla responsabilità civile per tali attività.

(36) I fabbricanti di prodotti con elementi digitali dovrebbero mettere in atto politiche di divulgazione coordinata delle vulnerabilità per facilitare la segnalazione delle vulnerabilità da parte di individui o soggetti ***direttamente al fabbricante o indirettamente nonché, qualora sia richiesto di procedere in forma anonima, tramite i CSIRT designati come coordinatori ai fini della divulgazione coordinata delle***

---

*[25] **Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (GU L 201 del 31.7.2002, pag. 37).***

vulnerabilità a norma dell'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555. Una politica di divulgazione coordinata delle vulnerabilità ***da parte dei fabbricanti*** 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").

(36 bis) Gli Stati membri e l'ENISA dovrebbero provvedere affinché le vulnerabilità segnalate in conformità del presente regolamento non siano utilizzate da organismi pubblici a fini di intelligence o di sorveglianza o a scopi offensivi.

(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 ***("software bill of materials" – SBOM)***. Tale distinta ***base del software*** 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. ***I fabbricanti non dovrebbero, tuttavia, essere obbligati a rendere pubblica la distinta base del software, in quanto ciò potrebbe avere conseguenze indesiderate sulla cibersicurezza dei loro prodotti con elementi digitali.***

(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[26]. Il regolamento (UE) n. 1025/2012 prevede una procedura di obiezione a norme armonizzate che non soddisfano completamente i requisiti del presente regolamento. ***Il processo di normazione dovrebbe garantire una rappresentazione equilibrata degli interessi e un'effettiva partecipazione dei portatori di interessi della società civile, comprese le organizzazioni dei consumatori. È opportuno tenere conto anche delle norme internazionali, in modo da semplificare lo sviluppo di norme armonizzate e l'attuazione del presente regolamento, nonché per ridurre gli ostacoli tecnici non tariffari agli scambi.***

(38 bis) Considerando l'ampio ambito di applicazione del presente regolamento, lo sviluppo tempestivo di norme armonizzate rappresenta una sfida significativa. La Commissione dovrebbe provvedere affinché siano in vigore norme armonizzate entro la data di applicazione del presente regolamento, in modo da garantirne l'efficace attuazione.

(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 ***fornire un quadro comune di fiducia per gli utilizzatori dei*** prodotti con elementi digitali contemplati dal presente regolamento. Il presente regolamento dovrebbe ***pertanto*** 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

[26] 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).

elementi digitali dovrebbero tenere conto dei requisiti essenziali stabiliti nel presente regolamento e facilitare la conformità a quest'ultimo. Alla Commissione dovrebbe essere conferito il potere di specificare, mediante atti ***delegati***, i sistemi europei di certificazione della cibersicurezza che possono essere utilizzati per dimostrare la conformità ***dei prodotti con elementi digitali*** ai requisiti essenziali stabiliti nel presente regolamento. Inoltre, al fine di evitare un onere amministrativo indebito a carico dei fabbricanti, ***non*** dovrebbe esistere ***alcun*** obbligo per i fabbricanti di effettuare una valutazione della conformità da parte di terzi, come previsto dal presente regolamento per i requisiti corrispondenti***, se è stato rilasciato un certificato di cibersicurezza nell'ambito di tali sistemi europei di certificazione della cibersicurezza, di un livello sostanziale o elevato***.

(39 bis) Al fine di agevolare il rispetto del presente regolamento, la Commissione dovrebbe aggiornare il programma di lavoro progressivo dell'Unione e chiedere all'ENISA di preparare le proposte di sistemi mancanti conformemente all'articolo 48 del regolamento (UE) 2019/881.

(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 ***delegati, dopo aver tenuto conto delle norme internazionali***. ***Tale opzione dovrebbe essere vista come una soluzione eccezionale "di ripiego", quando il processo di*** normazione ***è bloccato, quando vi sono*** ritardi ingiustificati nell'elaborazione di norme armonizzate

appropriate o ***quando i prodotti da fornire non sono conformi alla*** richiesta ***iniziale*** 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[27]. 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

---

[27] 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).

conformi a tali requisiti, è necessario prevedere procedure di valutazione della conformità. La decisione n. 768/2008/CE del Parlamento europeo e del Consiglio[28] 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 ***basata sul rischio e, nella maggior parte dei casi,*** 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 ***tali norme armonizzate, specifiche comuni o sistemi di certificazione della cibersicurezza sono in vigore da un periodo di tempo minimo atto a consentire ai fabbricanti di adottarle e il fabbricante*** non ***le*** applica, 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

[28] 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).

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.

(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***, in particolare per le microimprese e le piccole e medie imprese***. ***A tale proposito, gli Stati membri, con il sostegno della Commissione, dovrebbero garantire un'adeguata disponibilità di professionisti qualificati per far sì che gli organismi notificati possano svolgere le loro attività in modo efficiente, riducendo così al minimo possibili impedimenti, evitando***

strozzature e facilitando la conformità degli operatori economici al presente regolamento. 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.

53 bis) Per aumentare l'efficienza e la trasparenza, gli Stati membri dovrebbero garantire, prima della data di applicazione del presente regolamento, che nell'Unione vi sia un numero sufficiente di organismi notificati per eseguire le valutazioni della conformità. La Commissione dovrebbe monitorare gli sviluppi del mercato e assistere gli Stati membri in questo sforzo, al fine di evitare strozzature e ostacoli all'ingresso nel mercato.

(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[29] 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 ***alla*** direttiva ***(UE) 2022/2555*** 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

[29] 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).

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 la ciberresilienza dei prodotti con elementi digitali, ai fini dell'***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 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 ***alla*** direttiva ***(UE) 2022/255*** 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 ***alla*** direttiva ***(UE) 2022/2555***, 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 ***(UE) 2022/2555*** 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 ***dovrebbero*** essere organizzate indagini a tappeto, basandosi, tra l'altro, sulle notifiche ricevute riguardanti le vulnerabilità e gli incidenti relativi ai prodotti. ***La Commissione dovrebbe inoltre coordinare le autorità di vigilanza del mercato nelle ispezioni periodiche dei prodotti con elementi digitali che potrebbero presentare un rischio di sicurezza per l'Unione, anche alla luce del fattore di rischio non tecnico.***

(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 la specificazione dei 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 e*** 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. ***Alla Commissione dovrebbe inoltre essere delegato il potere di adottare atti delegati per specificare il formato e gli elementi della distinta base del software e specificare ulteriormente il formato e la procedura delle notifiche trasmesse all'ENISA dai fabbricanti riguardo alle vulnerabilità attivamente sfruttate e agli incidenti di rilievo. Ove necessario, alla Commissione dovrebbe essere conferito il potere di adottare atti delegati per adottare specifiche comuni per quanto riguarda i requisiti essenziali di cui all'allegato I.*** 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[30]. 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 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. ***Ai fini dell'elaborazione di atti delegati a norma del presente regolamento, la Commissione dovrebbe consultare il gruppo di esperti sulla ciberresilienza. La Commissione dovrebbe inoltre condurre un dialogo strutturale regolare con gli***

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

operatori economici ed effettuare consultazioni pubbliche, anche al fine di valutare l'ambito di applicazione del presente regolamento e l'opportunità di includere o escludere determinate categorie di prodotti.

(63) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, è opportuno attribuire alla Commissione competenze di esecuzione per: ▌ stabilire le specifiche tecniche per ***i sistemi di etichettatura, comprese etichette armonizzate,*** 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[31].

(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 ***il fabbricante sia una microimpresa, una piccola o media impresa o una start-up e*** 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

[31] 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).

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.

(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.

(66 bis) Le entrate generate dal pagamento delle sanzioni dovrebbero essere utilizzate per rafforzare il livello di cibersicurezza all'interno dell'Unione, anche attraverso lo sviluppo di capacità e competenze in materia di cibersicurezza, il miglioramento della ciberresilienza degli operatori economici, in particolare delle microimprese e delle piccole e medie imprese, e, più in generale, la sensibilizzazione del pubblico riguardo alle questioni di cibersicurezza.

(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 ***il gruppo di esperti e altre*** 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 [***36*** mesi] dopo la sua entrata in vigore, ad eccezione degli obblighi di segnalazione delle vulnerabilità attivamente sfruttate e degli incidenti, che dovrebbero applicarsi [***18*** mesi] dopo l'entrata in vigore del presente regolamento.

(69 bis) Il presente regolamento genererà costi aggiuntivi per le microimprese e le piccole e medie imprese, comprese le start-up. Per aiutare queste imprese, la Commissione dovrebbe istituire un sostegno finanziario e tecnico che consenta loro di contribuire alla crescita dell'economia europea e del panorama europeo della cibersicurezza, anche razionalizzando il sostegno finanziario del programma Europa digitale e di altri programmi pertinenti dell'Unione, nonché sostenendo le imprese e le organizzazioni del settore pubblico attraverso i poli europei di innovazione digitale. Inoltre, gli Stati membri dovrebbero prendere in considerazione tutte le possibili azioni complementari volte a fornire orientamento e sostegno alle microimprese e alle piccole e medie imprese, anche attraverso l'istituzione di spazi di sperimentazione normativa, poli di cibersicurezza e acceleratori di start-up.

(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[32] e ha espresso un parere il ***9 novembre 2022***[33].

(71 bis) La Commissione dovrebbe modificare la scheda finanziaria legislativa che accompagna il presente regolamento fornendo all'ENISA nove posti supplementari equivalenti a tempo pieno e stanziamenti supplementari corrispondenti per consentirle di svolgere i compiti aggiuntivi che le incombono a norma del presente regolamento.

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto

Il presente regolamento stabilisce:

a) norme per ***la messa a disposizione*** 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;

[32] 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).

[33] GU C 452 del 29.11.2022, pag. 23.

d) norme ***sul monitoraggio,*** 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 ***messi a disposizione sul mercato che possono avere*** una connessione dati ▌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 ***legislativi*** 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.

3 bis. Il presente regolamento si applica ai software liberi e open source solo se messi a disposizione sul mercato nel corso di un'attività commerciale.

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.

4 bis. Il presente regolamento non si applica ai pezzi di ricambio fabbricati esclusivamente per sostituire parti identiche e forniti dal fabbricante dei prodotti originali con elementi digitali.

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 ***per suo conto*** 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;

(4 bis) "cibersicurezza": la cibersicurezza quale definita all'articolo 2, punto 1, del regolamento (UE) 2019/881;

(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***, di monetizzazione*** 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;

(21 bis) "microimprese", "piccole imprese" e "medie imprese": le micro imprese, le piccole imprese e le medie imprese quali definite nella raccomandazione 2003/361/CE della Commissione[34];

(21 ter) "consumatore": qualsiasi persona fisica che, nelle circostanze di cui al presente regolamento, agisce per fini che non rientrano nell'esercizio della sua attività commerciale, imprenditoriale, artigianale o professionale;

(21 quater) "periodo di assistenza": il periodo durante il quale il fabbricante garantisce che le vulnerabilità del prodotto con elementi digitali siano gestite in modo efficace e conformemente ai requisiti essenziali di cui all'allegato I, sezione 2;

(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;

---

[34] ***Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese [notificata con il numero C(2003) 1422] (GU L 124 del 20.5.2003, pag. 36).***

(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***, esclusi gli aggiornamenti di sicurezza necessari che mirano ad attenuare le vulnerabilità***;

(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;

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

(35) "rischio ▌": il rischio ***quale*** definito all'articolo ***6, punto 9),*** della direttiva ***(UE) 2022/2555***;

(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" ***o "SBOM"***: 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 ***quale*** definita all'articolo ***6, punto 15),*** della direttiva ***(UE) 2022/2555***;

(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;

(39 bis) "incidente": un incidente quale definito all'articolo 6, punto 6), della direttiva (UE) 2022/2555;

(39 ter) "quasi incidente": un quasi incidente quale definito all'articolo 6, punto 5), della direttiva (UE) 2022/2555;

(39 quater) "minaccia informatica": una minaccia informatica quale definita all'articolo 2, punto 8, del regolamento (UE) 2019/881;

(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. ▌Gli Stati membri non impediscono la presentazione e l'uso di un ***prototipo di prodotto*** con elementi digitali non conforme al presente regolamento***, a condizione che la disponibilità di tale prodotto sia limitata nel tempo e nell'area geografica e che venga fornito esclusivamente per essere testato e, ove possibile, con un segno visibile che ne indichi la non conformità***.

3. Gli Stati membri non impediscono la messa a disposizione ***a titolo gratuito*** 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.

3 bis. Gli Stati membri, se del caso con il sostegno dell'ENISA, possono istituire ambienti di prova controllati per prodotti innovativi al fine di facilitarne lo sviluppo. In tale contesto è fornito un sostegno particolare alle microimprese e alle piccole e medie imprese, tra cui le start-up.

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, ***muniti dei necessari aggiornamenti di sicurezza e funzionalità***, 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.

L'integrazione di un prodotto di classe di criticità superiore non modifica il livello di criticità del prodotto in cui è integrato.

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. ***Il primo di tali atti delegati può essere adottato non prima di due anni dalla data di entrata in vigore del presente regolamento. Qualsiasi atto delegato successivo può essere adottato non prima dei due anni successivi.*** 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'***articolo 3*** della direttiva ***(UE) 2022/2555***.

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 ...*** [***6*** mesi ***dopo l'***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.

Qualora una nuova categoria di prodotti critici con elementi digitali sia aggiunta alla classe I o II di cui all'allegato III mediante un atto delegato a norma del paragrafo 2 del presente articolo, essa è soggetta alle pertinenti procedure di valutazione della conformità di cui all'articolo 24, paragrafi 2 e 3, del presente regolamento entro 12 mesi dalla data di adozione del relativo atto delegato.

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 un livello di affidabilità" elevato"*** a norma del regolamento (UE) 2019/881 per dimostrare la conformità ai requisiti essenziali di cui all'allegato I o a loro parti. ***L'obbligo di ottenere un certificato europeo di cibersicurezza si applica entro 12 mesi dall'adozione del pertinente atto delegato.***

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 ***all'articolo 3*** della direttiva ***(UE) 2022/2555***, 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.

5 bis. Alla Commissione è conferito il potere di adottare gli atti delegati di cui al paragrafo 5 del presente articolo non prima di 12 mesi dall'adozione del pertinente sistema europeo di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881.

Articolo 6 bis

Gruppo di esperti sulla ciberresilienza

1. Entro il ... [6 mesi dalla data di entrata in vigore del presente regolamento] la Commissione istituisce un gruppo di esperti sulla ciberresilienza ("gruppo di esperti"). Il gruppo di esperti è nominato dalla Commissione per un mandato triennale rinnovabile. La composizione del gruppo di esperti mira a rispettare un equilibrio di genere e geografico e comprende:

a) rappresentanti di ciascuno dei seguenti organi e agenzie:

i) Agenzia dell'Unione europea per la cibersicurezza;

i bis) Centro europeo di competenza per la cibersicurezza;

ii) Comitato europeo per la protezione dei dati;

iii) organismi europei di normalizzazione.

Se necessario, possono essere invitati rappresentanti di altre agenzie dell'Unione.

b) esperti che rappresentano gli operatori economici interessati, garantendo un'adeguata rappresentanza delle microimprese e delle piccole e medie imprese;

c) esperti che rappresentano la società civile, comprese le organizzazioni dei consumatori e la comunità libera e open source;

d) esperti nominati a titolo personale, in possesso di conoscenze e di comprovata esperienza nei settori interessati dal presente regolamento;

e) esperti che rappresentano il mondo accademico, compresi le università, gli istituti di ricerca e altre organizzazioni scientifiche, compresi soggetti con competenze globali.

2. Il gruppo di esperti fornisce consulenza alla Commissione in merito a quanto segue:

a) l'elenco dei prodotti critici con elementi digitali di cui all'allegato III, nonché l'eventuale necessità di aggiornare tale elenco;

b) l'attuazione dei sistemi europei di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881 e la possibilità di renderli obbligatori per i prodotti con elementi digitali altamente critici;

c) valutazioni non vincolanti dei prodotti con elementi digitali su richiesta di un'autorità di vigilanza del mercato che sta conducendo un'indagine a norma dell'articolo 43;

d) l'applicazione dei concetti pertinenti del nuovo quadro legislativo ai software, in particolare ai software liberi e open source;

e) gli elementi del regolamento che devono essere oggetto degli orientamenti di cui all'articolo 17 bis;

f) la disponibilità e la qualità delle norme europee e internazionali e la possibilità di integrarle o sostituirle con specifiche tecniche comuni;

g) la disponibilità in tutta l'Unione di professionisti qualificati nel settore della cibersicurezza, tra cui personale adeguato per effettuare valutazioni della conformità da parte di terzi a norma del presente regolamento;

h) l'eventuale necessità di modificare il presente regolamento.

Il gruppo di esperti traccia inoltre una mappatura delle tendenze a livello dell'Unione e degli Stati membri per quanto riguarda le vulnerabilità esistenti e quelle risolte con patch.

3. Il gruppo di esperti tiene conto dei pareri di un'ampia gamma di portatori di interessi e svolge i propri compiti con il massimo livello di professionalità, indipendenza, imparzialità e obiettività.

3 bis. La Commissione consulta il gruppo di esperti quando elabora atti delegati o di esecuzione basati sul presente regolamento.

3 ter. Il gruppo di esperti può fornire alle autorità di vigilanza del mercato valutazioni non vincolanti dei prodotti con elementi digitali per facilitare le indagini a norma dell'articolo 43.

4. Il gruppo di esperti è presieduto dalla Commissione e costituito conformemente alle norme orizzontali relative alla creazione e al funzionamento dei gruppi di esperti della Commissione. In tale contesto la Commissione può invitare esperti con competenze specifiche su base ad hoc.

5. Il gruppo di esperti svolge i propri compiti nel rispetto del principio della trasparenza. La Commissione pubblica sul suo sito web la composizione del gruppo di esperti, la dichiarazione di interessi dei suoi membri, una sintesi delle riunioni del gruppo di esperti e altri documenti pertinenti.

Articolo 6 ter

Migliorare le competenze in un ambiente digitale ciberresiliente

Ai fini del presente regolamento e per rispondere alla domanda di professionisti in grado di garantire la cibersicurezza dei prodotti con elementi digitali, la Commissione e gli Stati membri, in cooperazione con l'ENISA, garantiscono l'attuazione dei seguenti elementi:

a) programmi di istruzione e formazione nel settore della cibersicurezza e relativi percorsi professionali, che contribuiscano a rendere la forza lavoro nel settore della cibersicurezza più resiliente e inclusiva, anche in termini di genere e in linea con le esigenze delle imprese interessate, in particolare se tali imprese sono microimprese, piccole o medie imprese, comprese le start-up, o la pubblica amministrazione;

b) ***iniziative volte ad aumentare la collaborazione tra il settore privato, gli operatori economici, anche attraverso la riqualificazione o il miglioramento delle competenze dei dipendenti dei fabbricanti, i consumatori, gli erogatori di istruzione e formazione e gli Stati membri, ampliando le possibilità per i giovani di accedere a posti di lavoro in questo settore;***

c) ***strategie volte a migliorare la mobilità della forza lavoro, sviluppare le competenze in materia di cibersicurezza e creare strumenti organizzativi e tecnologici per sviluppare al massimo i talenti esistenti in materia di cibersicurezza.***

Articolo 7

Sicurezza generale dei prodotti

In deroga all'articolo 2, paragrafo 1, terzo comma, lettera b), del regolamento ***(UE) 2023/988***, 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 ***(UE) 2023/988***, il capo III, sezione 1, i capi V e VII e i capi da IX a XI del regolamento ***(UE) 2023/988*** 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 ***competenti*** 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.

3 bis. I fabbricanti di prodotti con elementi digitali classificati come sistemi di IA ad alto rischio conformemente al paragrafo 1 del presente articolo possono partecipare agli spazi di sperimentazione normativa per l'IA di cui all'articolo 53 del regolamento [regolamento sull'IA].

Articolo 9

Prodotti macchina

I prodotti macchina che rientrano nell'ambito di applicazione del regolamento ***(UE) 2023/1230***, che sono prodotti con elementi digitali ***o prodotti parzialmente completati 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 ***(UE)***

2023/1230, 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.

Articolo 9 bis

Appalti pubblici di prodotti con elementi digitali

1. Fatte salve le direttive 2014/24/UE[35] e 2014/25/UE[36] del Parlamento europeo e del Consiglio, gli Stati membri garantiscono, negli appalti di prodotti con elementi digitali, un elevato livello di cibersicurezza e un periodo di sostegno adeguato.

2. Gli Stati membri provvedono affinché i fabbricanti pongano rimedio alle vulnerabilità che interessano i prodotti con elementi digitali oggetto di appalti pubblici, anche mettendo tempestivamente a disposizione aggiornamenti di sicurezza.

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

---

35 ***Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).***

36 ***Direttiva 2014/25/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali e che abroga la direttiva 2004/17/CE (GU L 94 del 28.3.2014, pag. 243).***

gli incidenti di sicurezza e ridurre al minimo l'impatto di tali incidenti, anche in relazione alla salute e alla sicurezza degli utilizzatori.

2 bis. ***Sulla base della valutazione dei rischi di cibersicurezza, i fabbricanti determinano in che modo i requisiti essenziali di cui all'allegato I, sezione 1, sono applicabili al loro prodotto con elementi digitali. Essi includono la valutazione dei rischi nella documentazione tecnica di cui all'articolo 23.***

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. ***Spetta al fabbricante garantire*** che tali componenti non compromettano la sicurezza del prodotto con elementi digitali***, anche quando integra componenti di software liberi e open source che non sono stati immessi sul mercato nel corso di un'attività commerciale***.

Quando individuano una vulnerabilità in un componente, anche in un componente libero e open source, integrato nel prodotto con elementi digitali, i fabbricanti affrontano e correggono la vulnerabilità conformemente ai requisiti di gestione delle vulnerabilità di cui all'allegato I, sezione 2, e condividono le misure correttive adottate con la persona o il soggetto che si occupa della manutenzione del componente.

4 bis. ***Il fabbricante dei componenti fornisce al fabbricante del prodotto finale con elementi digitali le informazioni e la documentazione necessarie per soddisfare i requisiti del presente regolamento al momento della fornitura di tali componenti. Tali informazioni sono fornite gratuitamente.***

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, ***i fabbricanti determinano il periodo di sostegno durante il quale*** le vulnerabilità di tale prodotto ***sono*** gestite in modo efficace e in conformità dei requisiti essenziali di cui all'allegato I, sezione 2. ***In tal modo, il fabbricante garantisce che il periodo di sostegno sia proporzionato alla durata di vita prevista del prodotto e adeguato alla natura del prodotto e alle aspettative degli utenti, alla disponibilità dell'ambiente operativo e, se del caso, al periodo di sostegno dei componenti principali integrati nel prodotto con elementi digitali. A tal fine, su richiesta delle autorità di vigilanza del mercato, i fabbricanti mettono a disposizione informazioni sulla durata di vita prevista del prodotto da essi considerata al fine di determinare la durata del periodo di sostegno per il prodotto immesso sul mercato. Nel determinare il periodo di sostegno le autorità di vigilanza del mercato monitorano i prodotti con elementi digitali e garantiscono attivamente che i fabbricanti abbiano applicato tali criteri in modo adeguato, anche valutando le informazioni ricevute dai fabbricanti sulla durata di vita prevista del prodotto.***

Se del caso, il periodo di sostegno è chiaramente indicato sul prodotto, sul suo imballaggio o è incluso negli accordi contrattuali. In ogni caso, anche gli utilizzatori finali sono informati prima dell'acquisto in merito alla durata del periodo di sostegno.

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.

Ove possibile, per i prodotti di consumo con elementi digitali, tali procedure includono aggiornamenti automatici di sicurezza per impostazione predefinita. Gli utilizzatori dovrebbero mantenere la possibilità di disattivare tali aggiornamenti automatici di sicurezza.

I fabbricanti informano attivamente gli utilizzatori quando i loro prodotti con elementi digitali hanno raggiunto la fine del loro periodo di sostegno.

6 bis. Se il periodo di sostegno è inferiore a cinque anni e la gestione delle vulnerabilità è terminata, i fabbricanti possono fornire l'accesso al codice sorgente di tale prodotto con elementi digitali ad altre imprese che si impegnano a estendere la fornitura di servizi di gestione delle vulnerabilità, in particolare di aggiornamenti di sicurezza. L'accesso a tali codici sorgente è fornito solo se previsto da un accordo contrattuale. Tale accordo tutela la proprietà del prodotto con elementi digitali e impedisce la diffusione del codice sorgente al grande pubblico, a eccezione dei casi in cui tale codice è già stato fornito sulla base di una licenza libera e aperta.

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 a disposizione delle autorità di vigilanza del mercato per un periodo di ***almeno*** dieci anni dalla data di immissione sul mercato del prodotto con elementi digitali ***o per la durata del periodo di sostegno, a seconda di quale sia il periodo più lungo***.

Le autorità di vigilanza del mercato garantiscono la riservatezza e l'adeguata protezione delle informazioni contenute nella documentazione tecnica fornita dai fabbricanti a norma dell'articolo 52.

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

orizzontali o specifiche del settore, 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.

Se tali informazioni e istruzioni sono fornite in formato elettronico, i fabbricanti:

a) le presentano in un formato di facile utilizzo che consenta all'utilizzatore di consultarli online, scaricarli, salvarli su un dispositivo elettronico e stamparli;

b) garantiscono che siano accessibili online almeno durante il periodo di sostegno del prodotto 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 ***almeno*** per la durata ***del periodo di sostegno*** ▌, 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. ***Alla*** Commissione***, previa consultazione del gruppo di esperti e tenendo conto delle norme internazionali, è conferito il potere di adottare atti delegati conformemente all'articolo 50 per integrare il presente regolamento specificando*** il formato e gli elementi della distinta base del software di cui all'allegato I, sezione 2, punto 1. ▌

Articolo 11

Obblighi di segnalazione dei fabbricanti

1. Il fabbricante notifica all'ENISA▌ qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali ***conformemente al paragrafo 1 bis del presente articolo***. ▌ 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 ***12*** della direttiva ***(UE) 2022/2555*** e informa l'autorità di vigilanza del mercato in merito alla vulnerabilità notificata. ***Qualora a una vulnerabilità notificata non corrispondano misure correttive o di attenuazione, l'ENISA garantisce che le informazioni sulla vulnerabilità notificata siano condivise in conformità a rigorosi protocolli di sicurezza e in base al principio della necessità di sapere.***

1 bis. Le notifiche di cui al paragrafo 1 sono soggette alla procedura seguente:

a) un allarme rapido, senza indebito ritardo e comunque entro 24 ore dal momento in cui il fabbricante è venuto a conoscenza dell'esistenza di una vulnerabilità attivamente sfruttata, indicando se sono disponibili misure correttive note o di attenuazione del rischio raccomandate;

b) una notifica di vulnerabilità, senza indebito ritardo e comunque entro 72 ore dal momento in cui il fabbricante è venuto a conoscenza della vulnerabilità attivamente sfruttata, che, se del caso, aggiorna le informazioni generali di cui alla lettera a), indicando eventuali misure correttive o di attenuazione adottate, e indica una valutazione della portata della vulnerabilità, compresi la sua gravità e il suo impatto;

c) una relazione finale entro un mese dalla trasmissione della notifica di vulnerabilità a norma della lettera b), o quando è disponibile una misura correttiva, che comprenda almeno:

i) una descrizione della vulnerabilità, compresi la sua gravità e il suo impatto;

ii) se disponibili, informazioni relative a qualsiasi attore che abbia sfruttato o che sfrutti la vulnerabilità;

iii) informazioni dettagliate relative all'aggiornamento di sicurezza o ad altre misure correttive messe a disposizione per porre rimedio alla vulnerabilità.

1 ter. Dopo la messa a disposizione di un aggiornamento di sicurezza o l'adozione di un'altra forma di misure correttive o di attenuazione, l'ENISA aggiunge la vulnerabilità notificata a norma del paragrafo 1 del presente articolo alla banca dati europea delle vulnerabilità di cui all'articolo 12 della direttiva (UE) 2022/2555.

2. Il fabbricante notifica all'ENISA ▌ qualsiasi incidente ***significativo*** che abbia un impatto sulla sicurezza del prodotto con elementi digitali ***conformemente al paragrafo 2 ter del presente articolo***. 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 ***8*** della direttiva ***(UE) 2022/2555*** e informa l'autorità di vigilanza del mercato degli incidenti significativi notificati. La ***sola*** notifica ***non espone il soggetto che la effettua a una maggiore responsabilità***.

2 bis. Un incidente è considerato significativo ai sensi del paragrafo 2 se:

a) ha causato o è in grado di causare una grave perturbazione operativa della produzione o dei servizi per il fabbricante interessato, che potrebbe avere ripercussioni sulla sicurezza di un prodotto; o

b) ha interessato o può interessare altre persone fisiche o giuridiche causando considerevoli danni materiali o immateriali.

2 ter. Le notifiche di cui al paragrafo 2 sono soggette alla procedura seguente:

a) un allarme rapido, senza indebito ritardo, e comunque entro 24 ore dal momento in cui il fabbricante è venuto a conoscenza dell'incidente significativo, che, se del caso, indica se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o se può avere un impatto transfrontaliero;

b) una notifica di incidente, senza indebito ritardo, e comunque entro 72 ore dal momento in cui il fabbricante è venuto a conoscenza dell'incidente significativo, che, se del caso, aggiorna le informazioni di cui alla lettera a) e indica una valutazione iniziale dell'incidente significativo, compresi la sua gravità e il suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

c) una relazione finale entro un mese dalla trasmissione della notifica di incidente di cui alla lettera b), che comprenda almeno:

i) una descrizione dettagliata dell'incidente, compresi la sua gravità e il suo impatto;

ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;

iii) le misure di attenuazione adottate e in corso;

iv) se del caso, l'impatto transfrontaliero dell'incidente.

In caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d) del presente paragrafo, gli Stati membri provvedono affinché il fabbricante interessato fornisca una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente.

2 quater. I fabbricanti che hanno notificato incidenti significativi a norma del presente regolamento e che sono altresì identificati come soggetti essenziali o soggetti importanti ai sensi della direttiva (UE) 2022/2555 sono considerati conformi ai requisiti di cui all'articolo 23 della direttiva (UE) 2022/2555. L'ENISA trasmette le notifiche ricevute a norma del presente regolamento al CSIRT responsabile in conformità alla direttiva (UE) 2022/2555. Un soggetto può essere sanzionato una sola volta per la mancata osservanza di obblighi che si sovrappongono.

2 quinquies. Se necessario, l'ENISA o il CSIRT pertinente possono chiedere ai fabbricanti di fornire una relazione intermedia sui pertinenti aggiornamenti della situazione della vulnerabilità attivamente sfruttata o dell'incidente significativo.

2 sexies. I fabbricanti che rientrano nella definizione di microimprese o piccole o medie imprese sono esentati dall'applicazione del paragrafo 1 bis, lettera a), e del paragrafo 2 ter, lettera a).

3. L'ENISA trasmette alla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), istituita dall'articolo ***16*** della direttiva ***(UE) 2022/2555***, 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 ***interessati*** del prodotto con elementi digitali ***e, se del caso, tutti gli utilizzatori,*** in merito all'incidente ***significativo*** e, se necessario, ***all'attenuazione dei rischi e*** alle misure correttive che essi possono adottare per attenuarne l'impatto.

4 bis. L'ENISA provvede affinché le notifiche di cui ai paragrafi 1 e 2 siano trasmesse tramite canali di comunicazione e conservate in server atti a garantire il livello più elevato possibile di cibersicurezza e protezione da soggetti malintenzionati.

4 ter. Qualora sia necessario sensibilizzare il pubblico per evitare un incidente significativo o affrontare un incidente significativo in corso, o qualora la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico, dopo aver consultato il fabbricante interessato l'ENISA e, se opportuno, i CSIRT o le

autorità competenti degli Stati membri interessati, possono informare il pubblico riguardo all'incidente significativo o imporre al fabbricante di farlo.

5. La Commissione ***adotta atti delegati, conformemente all'articolo 50, per integrare il presente regolamento specificando*** ulteriormente il▌formato e la procedura di trasmissione delle notifiche a norma dei paragrafi 1 e 2. Tali atti ***delegati*** sono adottati ***entro il ... [12 mesi dalla data di entrata in vigore del presente regolamento]***.

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 ***14*** della direttiva ***(UE) 2022/2555***. La prima relazione di questo tipo è presentata entro 24 mesi dall'inizio dell'applicazione degli obblighi di cui ai paragrafi 1 e 2. ***L'ENISA integra le informazioni pertinenti tratte dalle sue relazioni tecniche nella sua relazione sullo stato della cibersicurezza nell'Unione, presentata a norma dell'articolo 18 della direttiva (UE) 2022/2555***.

6 bis. L'ENISA, previa consultazione del gruppo di esperti, istituisce un meccanismo di segnalazione digitale sicuro al fine di semplificare gli obblighi di segnalazione dei fabbricanti. Tale meccanismo funge da punto di accesso unico per gli obblighi di segnalazione a norma del presente regolamento e, ove possibile, di altre normative dell'Unione.

▌Articolo 11 bis

Notifica volontaria

1. Oltre agli obblighi di notifica di cui all'articolo 11, possono essere trasmesse all'ENISA notifiche su base volontaria da parte dei seguenti soggetti:

a) i fabbricanti, per quanto riguarda gli incidenti, le minacce informatiche e i quasi incidenti;

b) soggetti diversi da quelli menzionati alla lettera a), indipendentemente dal fatto che rientrino o meno nell'ambito di applicazione del presente regolamento, per quanto riguarda gli incidenti significativi e non, le minacce informatiche e i quasi incidenti;

c) qualsiasi soggetto, per quanto riguarda le vulnerabilità che possono essere incluse nella banca dati europea delle vulnerabilità di cui all'articolo 12 della direttiva (UE) 2022/2555.

2. L'ENISA tratta le notifiche di cui al paragrafo 1, lettera a), del presente articolo secondo la procedura di cui all'articolo 11. L'ENISA può trattare le notifiche obbligatorie in via prioritaria rispetto alle notifiche volontarie.

3. Al fine di semplificare le notifiche volontarie, è possibile trasmetterle attraverso il meccanismo di segnalazione digitale sicuro di cui all'articolo 11, paragrafo 6 bis.

4. Se del caso, l'ENISA garantisce la riservatezza e la protezione adeguata delle informazioni fornite dal soggetto notificante. Fatti salvi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, la segnalazione volontaria non ha l'effetto di imporre al soggetto notificante alcun obbligo aggiuntivo a cui non sarebbe stato sottoposto se non avesse trasmesso la notifica.

Articolo 11 ter

Punto di contatto unico per gli utilizzatori

1. Per facilitare le segnalazioni in merito alla sicurezza dei prodotti, i fabbricanti designano un punto di contatto unico che consenta agli utilizzatori di comunicare direttamente e rapidamente con loro, se del caso per via elettronica e in modo facilmente fruibile, anche consentendo agli utilizzatori del prodotto di scegliere i mezzi di comunicazione di cui all'allegato II, punto 1, che non si basino unicamente su strumenti automatizzati.

2. Oltre agli obblighi previsti dalla direttiva 2000/31/CE del Parlamento europeo e del Consiglio [37], i fabbricanti rendono pubbliche le informazioni necessarie agli utilizzatori finali per identificare facilmente i loro punti di contatto unici e comunicare senza difficoltà con essi. Tali informazioni sono facilmente accessibili e sono tenute aggiornate.

---

[37] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (GU L 178 del 17.7.2000, pag. 1).

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. ***Su richiesta, fornisce una copia del mandato alle autorità di vigilanza del mercato***. 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;

   a bis) qualora il rappresentante autorizzato abbia motivo di credere che il prodotto con elementi digitali in questione presenta un rischio di cibersicurezza, ne informa il fabbricante;

   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 ***in maniera efficace*** 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, ***la dichiarazione di conformità UE sia disponibile*** e ***il prodotto*** sia accompagnato dalle informazioni e dalle istruzioni per l'uso di cui all'allegato II;

c bis) tutti i documenti comprovanti il rispetto dei requisiti stabiliti nel presente articolo siano stati ricevuti dal fabbricante.

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.

Sulla base delle raccomandazioni mirate ricevute dalle autorità di vigilanza del mercato o dalla Commissione a norma degli articoli 43 e 45, l'importatore applica tali raccomandazioni, compresi il ritiro o il richiamo del prodotto. Inoltre, qualora ritenga o abbia motivo di credere che un prodotto con elementi digitali possa presentare un rischio di cibersicurezza alla luce di fattori di rischio non tecnici, l'importatore ritira o richiama tale prodotto. Gli importatori ne informano le autorità di vigilanza del mercato e la Commissione.

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 ***e, se disponibile, il sito web,*** ai quali possono essere contattati sul prodotto con elementi digitali oppure ▌ 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 ***chiedono*** immediatamente ***al fabbricante di adottare*** 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.

6 bis. Quando ***vengono a conoscenza di*** 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***, e abbiano trasmesso tutta la documentazione pertinente al distributore***.

3. Se un distributore ritiene o ha motivo di credere***, sulla base delle informazioni in suo possesso,*** 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***, sulla base delle informazioni in loro possesso,*** 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 ***chiedono al fabbricante di adottare*** 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.

4 bis. Quando ***vengono a conoscenza di*** 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***, sulla base delle informazioni in suo possesso,*** 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

Caso 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 ***e lo mette a disposizione sul mercato*** 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 ▌, 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.

Articolo 17 bis

Orientamenti

1. Al fine di creare chiarezza e certezza per le pratiche degli operatori economici, nonché di assicurarne la coerenza, la Commissione elabora e pubblica orientamenti per gli operatori economici, in cui illustra le modalità di applicazione del presente regolamento, con una particolare attenzione alle modalità per agevolare la conformità da parte delle microimprese e delle piccole e medie imprese.

2. Gli orientamenti sono pubblicati entro il ... [12 mesi dall'entrata in vigore del presente regolamento] e vengono aggiornate se necessario, in particolare alla luce di eventuali modifiche dell'elenco dei prodotti critici di cui all'allegato III. Essi comprendono almeno i seguenti elementi:

(a) una spiegazione dettagliata dell'ambito di applicazione del presente regolamento, con particolare attenzione alle soluzioni di elaborazione dati da remoto e al software libero e aperto;

(b) i criteri dettagliati utilizzati per determinare in che modo i prodotti con elementi digitali critici sono classificati nelle classi I o II di cui all'allegato III;

(c) l'interazione tra il presente regolamento e altre normative dell'Unione, in particolare per quanto riguarda la presunzione di conformità e la valutazione della conformità;

(d) orientamenti destinati ai fabbricanti riguardo alle modalità per effettuare la valutazione dei rischi di cibersicurezza di cui all'articolo 10, paragrafo 2, e all'applicabilità dei requisiti essenziali incluse, se disponibili, le migliori pratiche;

(e) orientamenti destinati ai fabbricanti su come determinare adeguatamente il periodo di sostegno per le diverse categorie di prodotti conformemente all'articolo 10, paragrafo 6;

(f) una spiegazione riguardo a come gestire gli obblighi di segnalazione a norma del presente regolamento o di altre normative dell'Unione;

(g) un elenco degli atti delegati e di esecuzione pubblicati dalla Commissione a norma del presente regolamento;

(h) orientamenti destinati agli Stati membri sulla non perseguibilità dei ricercatori in materia di sicurezza delle informazioni;

(i) orientamenti su ciò che costituisce una modifica sostanziale.

3. Nell'elaborare gli orientamenti a norma del presente articolo, la Commissione consulta il gruppo di esperti.

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.

In conformità dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, la Commissione chiede a una o più organizzazioni europee di normazione di elaborare norme armonizzate per i requisiti essenziali di cui all'allegato I del presente regolamento. Nel preparare la richiesta di normazione per il presente regolamento, la Commissione cerca di tenere conto delle norme internazionali esistenti o imminenti in materia di cibersicurezza, al fine di semplificare lo sviluppo delle norme armonizzate.

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 ***adottare*** atti ***delegati ai sensi dell'articolo 50, per integrare il presente regolamento specificando*** i sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 da utilizzare per dimostrare la conformità ***dei prodotti con elementi digitali critici*** ai

requisiti essenziali o a parti di essi di cui all'allegato I. Inoltre ***l'emissione di*** un certificato di cibersicurezza rilasciato nell'ambito di tali sistemi ***con un livello di affidabilità "sostanziale" o "elevato"*** 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). ▌

Articolo 19

Specifiche comuni

1. ▌ ***Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 50, al fine di integrare il presente regolamento, stabilendo specifiche comuni relative ai*** requisiti ***tecnici che forniscono i mezzi per*** soddisfare ***i requisiti di cui all'allegato I per i prodotti rientranti nell'ambito di applicazione del presente regolamento ove siano soddisfatte le seguenti condizioni:***

(a) la Commissione ha chiesto, a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, a una o più organizzazioni europee di normazione di elaborare una norma armonizzata per i requisiti essenziali di cui all'allegato I e la richiesta non è stata accettata, o i prodotti della normazione europea che rispondono a tale richiesta non sono ultimati entro una determinata scadenza a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, oppure i prodotti della normazione europea non sono conformi alla richiesta; nonché

(b) nessun riferimento a norme armonizzate che contemplano i requisiti essenziali pertinenti di cui all'allegato I del presente regolamento è stato pubblicato nella Gazzetta ufficiale dell'Unione europea conformemente al regolamento (UE) n. 1025/2012 e non si prevede la pubblicazione di tale riferimento entro un termine ragionevole.

2. Prima di preparare l'atto delegato, la Commissione informa il gruppo di esperti che ritiene soddisfatte le condizioni di cui al paragrafo 1. Nel preparare gli atti delegati, la Commissione tiene conto dei pareri del gruppo di esperti.

3. Qualora una norma armonizzata sia adottata da un organismo europeo di normazione e proposta alla Commissione per la pubblicazione del suo riferimento

nella Gazzetta ufficiale dell'Unione europea, la Commissione valuta la norma armonizzata conformemente al regolamento (UE) n. 1025/2012. Quando un riferimento a una norma armonizzata è pubblicato nella Gazzetta ufficiale dell'Unione europea, la Commissione abroga gli atti delegati corrispondenti di cui al paragrafo 1, o le parti di tali atti che riguardano gli stessi requisiti essenziali di cui all'allegato I al presente regolamento.

Articolo 20

Dichiarazione UE di conformità

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 ***opportunamente*** 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. ***In quest'ultimo caso, la sezione pertinente del sito web è facilmente e direttamente accessibile ai consumatori.***

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. ***Previa consultazione del gruppo di esperti, dell'apposito gruppo di cooperazione amministrativa (ADCO) e, ove necessario, di altre parti interessate,*** la Commissione può, mediante atti di esecuzione, stabilire specifiche tecniche per ***i sistemi di etichettatura, comprese le etichette armonizzate,*** i pittogrammi o qualsiasi altro marchio relativo alla sicurezza dei prodotti con elementi digitali***, il loro periodo di sostegno*** e meccanismi per promuoverne l'uso ***tra le imprese e i consumatori, nonché per sensibilizzare il pubblico in merito alla sicurezza dei prodotti con elementi digitali***. 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, ***almeno durante il periodo di sostegno*** .

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. ***La Commissione provvede affinché gli oneri amministrativi a carico delle microimprese e delle piccole e medie imprese siano proporzionati.***

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***;***

   c bis) un sistema europeo di certificazione della cibersicurezza adottato ai sensi del regolamento (UE) 2019/881 in conformità dell'articolo 18, paragrafo 4.

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 ***con un livello di affidabilità "sostanziale" o "elevato"*** 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.

2 bis. Le norme armonizzate, le specifiche comuni o i sistemi europei di certificazione della cibersicurezza sono in vigore per sei mesi prima dell'applicazione della procedura di valutazione della conformità di cui al paragrafo 2 del presente articolo. Nei sei mesi precedenti l'applicazione del paragrafo 2 del presente articolo o qualora non esistano norme armonizzate, specifiche comuni o sistemi europei di certificazione della cibersicurezza, i fabbricanti dimostrano la conformità del prodotto con elementi digitali critici di classe I di cui all'allegato III mediante la procedura di cui al paragrafo 1 del presente articolo.

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) un certificato europeo di cibersicurezza, nel quadro di un sistema europeo di certificazione della cibersicurezza con un livello di affidabilità "sostanziale" o "elevato" ai sensi del regolamento (UE) 2019/881;

(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.

3 bis. La Commissione chiede all'ENISA di preparare i sistemi candidati mancanti conformemente all'articolo 48 del regolamento (UE) 2019/881.

4. I fabbricanti di prodotti con elementi digitali classificati come sistemi di cartelle cliniche elettroniche che rientrano ***nel*** 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 ***micro,*** piccole e medie imprese ▌ 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. ***La Commissione garantisce un adeguato sostegno finanziario nel quadro normativo dei programmi dell'Unione esistenti, in particolare al fine di alleggerire l'onere finanziario per le microimprese e le piccole e medie imprese.***

Articolo 24 bis

Accordi di riconoscimento reciproco

Al fine di promuovere il commercio internazionale, la Commissione si adopera per concludere accordi di riconoscimento reciproco (ARR) con paesi terzi. L'Unione conclude ARR unicamente con i paesi terzi che presentano un livello comparabile di sviluppo tecnico e un approccio compatibile riguardo alla valutazione della conformità. Gli ARR assicurano lo stesso livello di protezione previsto dal presente regolamento.

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

Prescrizioni relative 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.

6 bis. L'autorità di notifica riduce al minimo gli oneri amministrativi e i diritti imposti, in particolare, alle microimprese e alle piccole e medie imprese.

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.

1 bis. Gli Stati membri garantiscono, entro ... [24 mesi dalla data di entrata in vigore del presente regolamento], che nell'Unione vi sia un numero sufficiente di organismi notificati per eseguire valutazioni della conformità, al fine di evitare strozzature e ostacoli all'ingresso nel mercato.

2. La Commissione rende pubbliche tali informazioni.

Articolo 29

Prescrizioni relative 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 ***di cui all'allegato I***, 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.

7 bis. Gli Stati membri e la Commissione mettono in atto misure adeguate onde garantire una disponibilità sufficiente di professionisti qualificati, al fine di ridurre al minimo gli ostacoli nelle attività degli organismi di valutazione della conformità e agevolare la conformità degli operatori economici al presente regolamento.

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 ***conformemente all'articolo 52***. 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 ***in conformità dell'articolo 37, paragrafo 2***, tenendo conto in particolare degli interessi delle ***microimprese e delle piccole e medie imprese*** 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***, tenendo conto delle microimprese e delle piccole e medie imprese***. 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 ***ed esposizione al rischio*** della tecnologia ***e del tipo di*** 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***, tenendo altresì conto della necessità di ridurre l'onere amministrativo e le tariffe***.

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***, le autorità competenti e i CSIRT designati a norma***

della direttiva (UE) 2022/2555, e procedono regolarmente a scambi di informazioni.

3 bis. ***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. Le autorità di vigilanza del mercato possono chiedere all'ENISA di fornire consulenza tecnica su questioni relative all'attuazione e all'applicazione del presente regolamento. Nel condurre un'indagine nel quadro dell'articolo 43, le autorità di vigilanza del mercato possono chiedere all'ENISA di fornire valutazioni non vincolanti sulla conformità dei prodotti con elementi digitali.***

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***, con competenze appropriate in materia di cibersicurezza,*** per svolgere i loro compiti a norma del presente regolamento.

7. La Commissione agevola lo scambio ***regolare e strutturato*** 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, ***come anche sui***

fattori di rischio non tecnici, con il sostegno ***dei CSIRT, dell'ENISA e*** della Commissione.

8 bis. Le autorità di vigilanza del mercato sono preparate a ricevere dai consumatori reclami a norma dell'articolo 11 del regolamento 2019/1020, anche istituendo meccanismi chiari e accessibili per agevolare la segnalazione di vulnerabilità, incidenti e minacce informatiche.

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.

Le autorità di vigilanza del mercato forniscono alla Commissione dati sul periodo di supporto medio stabilito dai fabbricanti, nonché, se disponibili, dati sulla durata media prevista del prodotto, disaggregati per categoria di prodotto con elementi digitali. La Commissione analizza tali informazioni e le pubblica in una banca dati accessibile al pubblico e di facile utilizzo.

9 bis. La Commissione valuta i dati segnalati anche a norma del paragrafo 9 del presente articolo, ai fini delle relazioni di cui all'articolo 56. Se i dati segnalati suggeriscono un aumento del livello di non conformità in specifiche categorie di prodotti, la Commissione, dopo aver consultato il gruppo di esperti e l'ADCO, può raccomandare che le autorità di vigilanza si concentrino maggiormente sulle categorie di prodotti interessate.

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 ▌ ADCO ***per la ciberresilienza dei prodotti con elementi digitali*** 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. ***In particolare, l'ADCO scambia le migliori pratiche e, se del caso, coopera con il gruppo di esperti e l'ENISA, come anche con il gruppo di cooperazione e la rete dei CSIRT di cui nella direttiva (UE) 2022/2555.***

11 bis. Le autorità di vigilanza del mercato facilitano il coinvolgimento dei portatori di interessi, comprese le organizzazioni scientifiche, di ricerca e di consumatori, nelle loro attività.

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***, senza indebito ritardo e, se del caso, in cooperazione con il CSIRT,*** 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 ***economico*** 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.

1 bis. Qualora l'autorità di vigilanza del mercato di uno Stato membro abbia motivi sufficienti per ritenere che un prodotto con elementi digitali presenti un rischio di cibersicurezza significativo o rappresenti una minaccia per la sicurezza nazionale alla luce di fattori di rischio non tecnici, essa formula raccomandazioni mirate destinate agli operatori economici volte a garantire l'adozione di 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, ***chiede*** alle autorità di vigilanza del mercato competenti di effettuare una valutazione della conformità e di seguire le procedure di cui all'articolo 43.

1 bis. Se la Commissione ha motivi sufficienti per ritenere che un prodotto con elementi digitali presenti un rischio di cibersicurezza significativo alla luce di fattori di rischio

non tecnici, essa informa le autorità di vigilanza del mercato competenti e formula raccomandazioni mirate destinate agli operatori economici volte a garantire l'adozione di opportune misure correttive.

2. In circostanze ▌ 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 ***chiede*** 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'***articolo 3*** della direttiva ***(UE) 2022/2555*** o per altri aspetti della tutela dell'interesse pubblico, essa chiede all'operatore ***economico*** 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 ***economici*** 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 ▌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 ***stabilisce, se necessario,*** 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 ***realizzano*** 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 ***propongono*** 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 ***conducono regolarmente e*** 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. ***Esse comprendono ispezioni su prodotti acquistati sotto un'identità di copertura e mirano a verificare la conformità di tali prodotti al presente regolamento.***

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 ***mette*** a disposizione del pubblico i risultati aggregati.

3. L'ENISA ***individua***, 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 ***sono*** 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 ***invitano*** 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 10, paragrafo 15, all'articolo 11, paragrafo 5, all'articolo 18, paragrafo 4, all'articolo 19, paragrafo 1,*** 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 10, paragrafo 15, all'articolo 11, paragrafo 5, all'articolo 18, paragrafo 4, all'articolo 19, paragrafo 1,*** 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 10, paragrafo 15, dell'articolo 11, paragrafo 5, dell'articolo 18, paragrafo 4, dell'articolo 19, paragrafo 1,*** dell'articolo 20, paragrafo 5, ***o*** 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[38];

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

[38] 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).

(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 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. ***Gli Stati membri provvedono affinché tali norme tengano conto delle capacità finanziarie delle microimprese e delle piccole e medie imprese.***

2. Gli Stati membri notificano tali norme e misure alla Commissione, senza indugio, e provvedono poi a dare immediata notifica delle eventuali modifiche successive. ***La Commissione provvede affinché tali norme e misure siano applicate in modo uniforme e coerente in tutta l'Unione.***

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;

(a bis) il carattere non intenzionale della violazione;

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

(c) le dimensioni***, in particolare per quanto riguarda le microimprese e le piccole e medie imprese, start up comprese,*** 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.

Articolo 53 bis

Destinazione delle entrate derivanti dalle sanzioni

Gli Stati membri destinano le entrate derivanti dalle sanzioni di cui all'articolo 53, paragrafo 1, a progetti che aumentano il livello di cibersicurezza all'interno dell'Unione. Tali progetti mirano al raggiungimento di almeno uno dei seguenti obiettivi:

(a) aumentare il numero dei professionisti qualificati nel settore della cibersicurezza, in particolare donne;

(b) aumentare lo sviluppo di capacità per le microimprese e le piccole e medie imprese al fine di facilitare la loro conformità al presente regolamento;

(c) migliorare la consapevolezza del pubblico in merito alle minacce informatiche, in particolare per quanto riguarda la loro prevenzione e gestione;

(d) sviluppare strumenti volti ad accrescere la resilienza delle imprese dell'Unione ai furti di proprietà intellettuale favoriti dall'informatica.

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 54 bis

Modifica della direttiva (UE) 2020/1828

Nell'allegato I della direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio[39] è aggiunto il seguente punto:

"67. [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].

3 bis. Fino alla data di applicazione del presente regolamento, i fabbricanti possono soddisfare i requisiti del presente regolamento su base volontaria. Se i fabbricanti si conformano al presente regolamento per quanto riguarda i loro prodotti con elementi digitali, essi sono considerati conformi anche al regolamento delegato (UE) 2022/30.

---

[39] Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (GU L 409 del 4.12.2020, pag. 1).

La Commissione abroga il regolamento delegato (UE) 2022/30 alla stessa data di applicazione del presente regolamento.

Articolo 56

Valutazione e riesame

1. 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.

2. ***Ogni anno, al momento della presentazione del progetto di bilancio per l'esercizio successivo, la Commissione presenta una valutazione dettagliata dei compiti dell'ENISA nel quadro del presente regolamento, come indicato nell'allegato VI bis e in altre pertinenti normative dell'Unione, e specifica le risorse finanziarie e umane necessarie per svolgere tali compiti.***

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 [***36*** mesi dopo la data della sua entrata in vigore]. Tuttavia l'articolo 11 si applica a partire dal [***18*** 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 ...▌ ,

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

ALLEGATO I

REQUISITI ESSENZIALI DI CIBERSICUREZZA

1. REQUISITI DI SICUREZZA RELATIVI ALLE PROPRIETÀ DEI PRODOTTI CON ELEMENTI DIGITALI

1) I prodotti con elementi digitali sono progettati, sviluppati e prodotti in modo da garantire un livello adeguato di cibersicurezza in base ai rischi.

▌

3) Sulla base della valutazione dei rischi ***di cibersicurezza*** di cui all'articolo 10, paragrafo 2, e ove applicabile, i prodotti con elementi digitali:

-a) sono messi a disposizione senza vulnerabilità sfruttabili note;

(a) sono ***messi a disposizione*** con una configurazione sicura per impostazione predefinita, ***salvo diversamente convenuto tra le parti in un contesto da impresa a impresa,*** con la possibilità di ripristinare il prodotto allo stato originale ***mantenendo tutti gli aggiornamenti di sicurezza***;

a bis) se tecnicamente fattibile, sono messi a disposizione sul mercato con una separazione funzionale degli aggiornamenti di sicurezza da quelli delle funzionalità;

a ter) garantiscono aggiornamenti automatici di sicurezza, con un meccanismo di opt-out chiaro e di facile utilizzo e la notifica agli utilizzatori degli aggiornamenti disponibili;

b) garantiscono la protezione dall'accesso non autorizzato mediante adeguati meccanismi di controllo, tra cui, a titolo esemplificativo ma non esaustivo, sistemi di autenticazione e di gestione dell'identità o dell'accesso;

c) proteggono la riservatezza dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, criptando i pertinenti dati a riposo o in transito mediante meccanismi all'avanguardia ***e utilizzando altri mezzi tecnici***;

d) proteggono l'integrità dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, dei comandi, dei programmi e della configurazione da qualsiasi manipolazione o modifica non autorizzata da parte dell'utilizzatore, e segnalano le corruzioni ***o possibili accessi non autorizzati***;

e) trattano solo dati, personali o di altro tipo, adeguati, pertinenti e limitati a quanto necessario in relazione all'uso previsto del prodotto ("minimizzazione dei dati");

f) proteggono la disponibilità delle funzioni essenziali ***e di base***, ***anche dopo un incidente,*** comprese ***la gestione del backup e le misure di*** resilienza e attenuazione ***contro gli*** attacchi di negazione del servizio (denial of service);

g) riducono al minimo il loro impatto negativo sulla disponibilità dei servizi forniti da altri dispositivi o reti;

h) sono progettati, sviluppati e prodotti per limitare le superfici di attacco, comprese le interfacce esterne;

i) sono progettati, sviluppati e prodotti per ridurre l'impatto degli incidenti utilizzando meccanismi e tecniche di attenuazione dello sfruttamento adeguati;

j) forniscono informazioni sulla sicurezza registrando e/o monitorando le ***capacità relative alle*** attività interne pertinenti, compresi l'accesso a dati, servizi o funzioni o la modifica degli stessi***, con meccanismi di opt-out per l'utilizzatore***;

I

k bis) consentono agli utilizzatori di ritirare ed eliminare i loro dati in modo permanente.

2. REQUISITI DI GESTIONE DELLE VULNERABILITÀ

I fabbricanti di prodotti con elementi digitali:

1) identificano e documentano le vulnerabilità e i componenti contenuti nel prodotto, redigendo anche una distinta base del software in un formato di uso comune e leggibile da un dispositivo automatico, che includa almeno le dipendenze di primo livello del prodotto;

2) in relazione ai rischi posti dai prodotti con elementi digitali, affrontano e correggono tempestivamente le vulnerabilità, anche fornendo aggiornamenti di sicurezza***, installati automaticamente ove applicabile in conformità della sezione I***;

3) effettuano prove e riesami efficaci e periodici della sicurezza del prodotto con elementi digitali;

4) una volta reso disponibile un aggiornamento di sicurezza, ***condividono e*** divulgano pubblicamente informazioni sulle vulnerabilità risolte ***in modo controllato***, compresi una descrizione delle vulnerabilità, informazioni che consentano agli utilizzatori di identificare il prodotto con elementi digitali interessato, l'impatto delle vulnerabilità, la loro gravità e informazioni ***chiare e accessibili*** che aiutino gli utilizzatori a correggere le vulnerabilità;

5) mettono in atto e applicano una politica di divulgazione coordinata delle vulnerabilità;

6) adottano misure per facilitare la condivisione di informazioni sulle potenziali vulnerabilità nel loro prodotto con elementi digitali e nei componenti di terzi contenuti in tale prodotto, fornendo anche un indirizzo di contatto per la segnalazione delle vulnerabilità individuate nel prodotto con elementi digitali;

7) prevedono meccanismi per distribuire in modo sicuro gli aggiornamenti ***di sicurezza*** dei prodotti con elementi digitali, per garantire che le vulnerabilità sfruttabili siano corrette o attenuate in modo tempestivo;

8) garantiscono che, qualora disponibili, siano diffusi tempestivamente e gratuitamente***, salvo diversamente convenuto tra le parti in un contesto da impresa a impresa,*** patch o aggiornamenti di sicurezza per risolvere i problemi di sicurezza individuati, accompagnati da messaggi di avviso che forniscano agli utilizzatori le informazioni pertinenti, comprese le potenziali misure da adottare***.***

8 bis) ove possibile e applicabile, notificano all'utilizzatore la fine del periodo di supporto.

ALLEGATO II

INFORMAZIONI E ISTRUZIONI PER L'UTILIZZATORE

Il prodotto con elementi digitali è accompagnato, come minimo, dagli elementi seguenti:

1. il nome, la denominazione commerciale registrata o il marchio registrato del fabbricante, l'indirizzo postale e l'indirizzo di posta elettronica ***e se disponibile il sito web*** a cui il fabbricante può essere contattato, indicati sul prodotto oppure ▌ sull'imballaggio o in un documento di accompagnamento;
2. il punto di contatto ***unico*** dove è possibile segnalare e ricevere informazioni sulle vulnerabilità di cibersicurezza del prodotto ***e sulla politica del fabbricante in materia di vulnerabilità coordinate e su dove la si può trovare***;
3. la corretta identificazione del tipo, del lotto, della versione o del numero di serie o di altri elementi che consentano l'identificazione del prodotto e delle relative istruzioni e informazioni per l'utilizzatore;
4. l'uso previsto, compreso l'ambiente di sicurezza fornito dal fabbricante, nonché le funzionalità essenziali del prodotto e le informazioni sulle proprietà di sicurezza;
5. qualsiasi circostanza nota o prevedibile connessa all'uso del prodotto con elementi digitali in conformità alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, che possa comportare rischi di cibersicurezza significativi;
6. se e, ove applicabile, dove è possibile ***per le autorità competenti*** accedere alla distinta base del software ***in conformità delle condizioni di non divulgazione di cui all'articolo 52***;
7. se del caso, l'indirizzo internet dove è possibile accedere alla dichiarazione di conformità UE;
8. il tipo di assistenza tecnica di sicurezza offerta dal fabbricante e ***il periodo di supporto durante il quale*** gli utilizzatori possono aspettarsi ***che le vulnerabilità siano trattate e*** di ricevere gli aggiornamenti di sicurezza;
9. istruzioni dettagliate o un indirizzo internet che rimandi a tali istruzioni e informazioni su quanto segue:
   (a) le misure necessarie durante la prima messa in servizio e per tutta la durata del prodotto per garantirne l'uso sicuro;
   (b) in che modo le modifiche del prodotto possono influire sulla sicurezza dei dati;
   (c) le modalità di installazione degli aggiornamenti rilevanti per la sicurezza;
   (d) lo smantellamento sicuro del prodotto, comprese le informazioni sulle modalità di eliminazione sicura dei dati degli utilizzatori.

ALLEGATO III

PRODOTTI CON ELEMENTI DIGITALI CRITICI

Classe I

1. Software per sistemi di gestione dell'identità e software per la gestione degli accessi privilegiati;
2. browser autonomi e incorporati;
3. sistemi di gestione delle password;

3 bis. lettori biometrici;

4. software che cercano, rimuovono o mettono in quarantena i software maligni;
5. prodotti con elementi digitali con funzione di rete privata virtuale (VPN);
6. sistemi di gestione della rete;
7. strumenti di gestione della configurazione di rete;
8. sistemi di monitoraggio del traffico di rete;
9. gestione delle risorse di rete;
10. sistemi di gestione delle informazioni e degli eventi di sicurezza (sistemi SIEM);
11. gestione di patch/aggiornamenti, compresi i boot manager;
12. sistemi di gestione della configurazione delle applicazioni;
13. software per l'accesso remoto;
14. software per la gestione dei dispositivi mobili;
15. interfacce di rete fisiche ***e virtuali***;
16. sistemi operativi non compresi nella classe II;
17. firewall, sistemi di rilevamento e/o prevenzione delle intrusioni non compresi nella classe II;
19. ***microprocessori di uso generale e*** microprocessori non compresi nella classe II;
20. microcontrollori;
21. circuiti integrati per applicazioni specifiche (ASIC) e reti di porte programmabili dall'utilizzatore (FPGA) destinati all'uso da parte di soggetti essenziali del tipo indicato ***all'articolo 3*** della direttiva ***(UE) 2022/2555***;
22. sistemi di controllo per l'automazione industriale (IACS) non compresi nella classe II, come i controllori logici programmabili (PLC), i sistemi di controllo distribuito (DCS), i controllori numerici computerizzati per macchine utensili (CNC)***, i robot industriali e i loro sistemi di controllo*** e i sistemi di controllo di supervisione e acquisizione dati (SCADA);
23. internet delle cose industriale non rientrante nella classe II***;***

23 bis. sistemi domotici, tra cui i server per case intelligenti e gli assistenti virtuali;

23 ter. dispositivi di sicurezza, tra cui serrature, telecamere e sistemi di allarme intelligenti;

23 quater. giocattoli intelligenti;

23 quinquies. apparecchiature sanitarie personali e dispositivi indossabili.

Classe II

1. Sistemi operativi per server, desktop e dispositivi mobili;
2. ipervisori e sistemi di runtime container che supportano l'esecuzione virtualizzata di sistemi operativi e ambienti simili;
3. infrastrutture a chiave pubblica ed emittenti di certificati digitali;
4. firewall, sistemi di rilevamento e/o prevenzione delle intrusioni destinati all'uso industriale;

▌

6. microprocessori destinati all'integrazione in controllori logici programmabili ed elementi sicuri;
7. router, modem per la connessione a internet e switch ▌;
8. elementi sicuri;
9. moduli di sicurezza dell'hardware (HSM);
10. criptoprocessori sicuri;
11. carte intelligenti, lettori di carte intelligenti e token;
12. sistemi di controllo per l'automazione industriale (IACS) destinati all'uso da parte di soggetti essenziali del tipo di cui all'***articolo 3*** della direttiva ***(UE) 2022/2555*** come i controllori logici programmabili (PLC), i sistemi di controllo distribuito (DCS), i controllori numerici computerizzati per macchine utensili (CNC) e i sistemi di controllo di supervisione e acquisizione dati (SCADA);
13. dispositivi dell'internet delle cose industriale destinati all'uso da parte di soggetti essenziali del tipo indicato ***all'articolo 3*** della direttiva ***(UE) 2022/2555***;

▌

15. contatori intelligenti.

ALLEGATO IV

DICHIARAZIONE DI CONFORMITÀ UE

La dichiarazione di conformità UE di cui all'articolo 20 contiene tutte le informazioni seguenti:

1. nome e tipo e qualsiasi altra informazione che consenta l'identificazione univoca del prodotto con elementi digitali;
2. nome e indirizzo del fabbricante o del suo rappresentante autorizzato;
3. un'attestazione secondo cui la dichiarazione di conformità UE è rilasciata sotto la responsabilità esclusiva del fornitore;
4. oggetto della dichiarazione (identificazione del prodotto che ne consenta la tracciabilità. Può, se del caso, includere una fotografia);
5. un'attestazione secondo la quale l'oggetto della dichiarazione di cui sopra è conforme alla pertinente normativa di armonizzazione dell'Unione;
6. riferimenti alle pertinenti norme armonizzate utilizzate o a qualsiasi altra specifica comune o certificazione di cibersicurezza in relazione alla quale è dichiarata la conformità;
7. ove applicabile, il nome e il numero dell'organismo notificato, una descrizione della procedura di valutazione della conformità applicata e l'identificazione del certificato rilasciato;
8. informazioni supplementari:

Firmato a nome e per conto di: ……

(luogo e data del rilascio):

(nome, funzione) (firma):

ALLEGATO V

CONTENUTI DELLA DOCUMENTAZIONE TECNICA

La documentazione tecnica di cui all'articolo 23 include almeno le informazioni seguenti, a seconda dell'applicabilità al pertinente prodotto con elementi digitali:

1. una descrizione generale del prodotto con elementi digitali, tra cui:
   a) la finalità prevista;
   b) versioni del software importanti per la conformità ai requisiti essenziali;
   c) se il prodotto con elementi digitali consiste di un prodotto hardware, fotografie o illustrazioni che mostrino le caratteristiche esterne, la marcatura e la disposizione interna;
   d) informazioni e istruzioni per l'utilizzatore, come indicato nell'allegato II;
2. una descrizione della progettazione, dello sviluppo e della produzione del prodotto e dei processi di gestione delle vulnerabilità, tra cui:
   a) informazioni complete sulla progettazione e sullo sviluppo del prodotto con elementi digitali, compresi, se del caso, disegni e schemi e/o una descrizione dell'architettura del sistema che spieghi in che modo i componenti software si basano l'uno sull'altro o si alimentano reciprocamente e si integrano nel processo complessivo;
   b) informazioni complete e specifiche sui processi di gestione delle vulnerabilità messi in atto dal fabbricante, tra cui la distinta base del software, la politica di gestione della divulgazione coordinata delle vulnerabilità, la prova della fornitura di un indirizzo di contatto per la segnalazione delle vulnerabilità e una descrizione delle soluzioni tecniche scelte per la distribuzione sicura degli aggiornamenti;
   c) informazioni complete e specifiche relative ai processi di produzione e monitoraggio del prodotto con elementi digitali e alla convalida di tali processi;
3. una valutazione dei rischi di cibersicurezza a fronte dei quali il prodotto con elementi digitali è progettato, sviluppato, prodotto, consegnato e sottoposto a manutenzione, come stabilito all'articolo 10 del presente regolamento***, incluse le modalità di applicazione dei requisiti essenziali di cui all'allegato I, sezione 1***;
4. un elenco delle norme armonizzate applicate integralmente o in parte, i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, delle specifiche comuni di cui all'articolo 19 del presente regolamento o dei sistemi di certificazione della cibersicurezza di cui al regolamento (UE) 2019/881 a norma dell'articolo 18, paragrafo 3, e, qualora non siano stati applicati tali norme armonizzate, specifiche comuni o sistemi di certificazione della cibersicurezza, le descrizioni delle soluzioni adottate per soddisfare i requisiti essenziali di cui all'allegato I, sezioni 1 e 2, compreso un elenco delle altre pertinenti specifiche tecniche applicate. In caso di applicazione parziale delle norme armonizzate, delle specifiche comuni o delle certificazioni di cibersicurezza, la documentazione tecnica specifica le parti che sono state applicate;

5. le relazioni delle prove effettuate per verificare la conformità del prodotto e dei processi di gestione delle vulnerabilità ai requisiti essenziali applicabili di cui all'allegato I, sezioni 1 e 2;

6. una copia della dichiarazione di conformità UE;

7. se del caso, la distinta base del software quale definita all'articolo 3, punto 36, a seguito di una richiesta motivata di un'autorità di vigilanza del mercato, a condizione che ciò sia necessario affinché tale autorità possa verificare la conformità ai requisiti essenziali di cui all'allegato I.

ALLEGATO VI

PROCEDURE DI VALUTAZIONE DELLA CONFORMITÀ

Procedura di valutazione della conformità basata sul controllo interno (basata sul modulo A)

1. Il controllo interno è la procedura di valutazione della conformità con cui il fabbricante adempie agli obblighi di cui ai punti 2, 3 e 4 e garantisce e dichiara, sotto la sua esclusiva responsabilità, che i prodotti con elementi digitali soddisfano tutti i requisiti essenziali di cui all'allegato I, sezione 1, e che il fabbricante soddisfa i requisiti essenziali di cui all'allegato I, sezione 2.

2. Il fabbricante redige la documentazione tecnica di cui all'allegato V.

3. Progettazione, sviluppo, produzione e gestione delle vulnerabilità dei prodotti con elementi digitali

   Il fabbricante adotta tutte le misure necessarie affinché i processi di progettazione, sviluppo, produzione e gestione delle vulnerabilità e il loro monitoraggio garantiscano la conformità dei prodotti con elementi digitali fabbricati o sviluppati e dei processi messi in atto dal fabbricante ai requisiti essenziali di cui all'allegato I, sezioni 1 e 2.

4. Marcatura di conformità e dichiarazione di conformità

4.1. Il fabbricante appone la marcatura CE ad ogni singolo prodotto con elementi digitali che soddisfa i requisiti applicabili del presente regolamento.

4.2. Per ciascun prodotto con elementi digitali il fabbricante compila una dichiarazione di conformità UE scritta in conformità dell'articolo 20 che, insieme alla documentazione tecnica, lascia a disposizione delle autorità nazionali per dieci anni dalla data in cui il prodotto con elementi digitali è stato immesso sul mercato ***o per il periodo di supporto, se quest'ultimo è superiore***. La dichiarazione di conformità UE identifica il prodotto con elementi digitali per cui è stata compilata. Una copia della dichiarazione di conformità UE è messa a disposizione delle autorità competenti su richiesta.

5. Rappresentanti autorizzati

   Gli obblighi del fabbricante previsti al punto 4 possono essere adempiuti dal suo rappresentante autorizzato, a nome del fabbricante e sotto la sua responsabilità, purché siano specificati nel mandato.

Esame UE del tipo (basato sul modulo B)

1. L'esame UE del tipo è la parte di una procedura di valutazione della conformità in cui un organismo notificato esamina la progettazione tecnica e lo sviluppo di un prodotto e i processi di gestione delle vulnerabilità messi in atto dal fabbricante e attesta che un prodotto con elementi digitali soddisfa i requisiti essenziali di cui all'allegato I, sezione 1, e che il fabbricante soddisfa i requisiti essenziali di cui all'allegato I, sezione 2.

2. L'esame UE del tipo è realizzato in base a una valutazione dell'adeguatezza della progettazione tecnica e dello sviluppo del prodotto, effettuata esaminando la documentazione tecnica e di supporto di cui al punto 3, unita all'esame di campioni di

una o più parti critiche del prodotto (combinazione tra tipo di produzione e tipo di progetto).

3. Il fabbricante presenta una domanda di esame UE del tipo a un unico organismo notificato di sua scelta.

La domanda contiene:

– il nome e l'indirizzo del fabbricante e, qualora la domanda sia presentata dal suo rappresentante autorizzato, il nome e l'indirizzo di quest'ultimo;

– una dichiarazione scritta in cui si precisa che la stessa domanda non è stata presentata a nessun altro organismo notificato;

– la documentazione tecnica, che consente di valutare la conformità del prodotto ai requisiti essenziali applicabili di cui all'allegato I, sezione 1, e dei processi di gestione delle vulnerabilità messi in atto dal fabbricante ai requisiti di cui all'allegato I, sezione 2, e che include un'analisi e una valutazione adeguate dei rischi. Essa precisa i requisiti applicabili e comprende, nella misura necessaria ai fini della valutazione, il progetto, la fabbricazione e il funzionamento del prodotto. La documentazione tecnica contiene, laddove applicabile, almeno gli elementi di cui all'allegato V;

– la documentazione di supporto attestante l'adeguatezza delle soluzioni di progettazione tecnica e sviluppo e dei processi di gestione delle vulnerabilità. Tale documentazione di supporto elenca tutti i documenti che sono stati utilizzati, soprattutto nel caso in cui le norme armonizzate e/o le specifiche tecniche pertinenti non siano state applicate integralmente. La documentazione di supporto comprende, ove necessario, i risultati delle prove effettuate dall'apposito laboratorio del fabbricante o da un altro laboratorio di prova, per conto e sotto la responsabilità del fabbricante.

4. L'organismo notificato:

4.1. esamina la documentazione tecnica e di supporto per valutare l'adeguatezza della progettazione tecnica e dello sviluppo del prodotto ai requisiti essenziali di cui all'allegato I, sezione 1, e dei processi di gestione delle vulnerabilità messi in atto dal fabbricante ai requisiti essenziali di cui all'allegato I, sezione 2;

4.2. verifica che i campioni siano stati sviluppati o fabbricati in conformità della documentazione tecnica e individua gli elementi progettati e sviluppati in conformità delle disposizioni applicabili delle norme armonizzate e/o delle specifiche tecniche pertinenti, nonché gli elementi progettati e sviluppati senza applicare le disposizioni pertinenti previste da tali norme;

4.3. effettua o fa effettuare esami e prove appropriati per controllare se, qualora il fabbricante abbia scelto di applicare le soluzioni di cui alle norme armonizzate e/o alle specifiche tecniche pertinenti per i requisiti di cui all'allegato I, tali soluzioni siano state applicate correttamente;

4.4. effettua o fa effettuare esami e prove appropriati per controllare se, laddove non siano state applicate le soluzioni di cui alle norme armonizzate e/o alle specifiche tecniche pertinenti per i requisiti di cui all'allegato I, le soluzioni adottate dal fabbricante soddisfino i requisiti essenziali corrispondenti;

4.5. concorda con il fabbricante il luogo in cui dovranno essere effettuati gli esami e le prove.

5. L'organismo notificato redige una relazione di valutazione che elenca le iniziative intraprese in conformità del punto 4 e i relativi risultati. Senza pregiudicare i propri obblighi di fronte alle autorità di notifica, l'organismo notificato rende pubblico l'intero contenuto della relazione, o parte di esso, solo con l'accordo del fabbricante.

6. Se il tipo e i processi di gestione delle vulnerabilità soddisfano i requisiti essenziali di cui all'allegato I, l'organismo notificato rilascia al fabbricante un certificato di esame UE del tipo. Il certificato indica nome e indirizzo del fabbricante, le conclusioni dell'esame, le eventuali condizioni di validità e i dati necessari per identificare il tipo omologato e i processi di gestione delle vulnerabilità. Il certificato può avere uno o più allegati.

   Il certificato e i suoi allegati contengono tutte le informazioni pertinenti per consentire la valutazione della conformità dei prodotti fabbricati o sviluppati al tipo esaminato e dei processi di gestione delle vulnerabilità e permettere il controllo dei prodotti in funzione.

   Se il tipo e i processi di gestione delle vulnerabilità non soddisfano i requisiti essenziali applicabili di cui all'allegato I, l'organismo notificato rifiuta di rilasciare un certificato di esame UE del tipo e informa di tale decisione il richiedente, motivando dettagliatamente il suo rifiuto.

7. L'organismo notificato segue l'evoluzione del progresso tecnologico generalmente riconosciuto, in base al quale il tipo omologato e i processi di gestione delle vulnerabilità potrebbero non essere più conformi ai requisiti essenziali applicabili di cui all'allegato I del presente regolamento, e decide se tale progresso richieda ulteriori indagini. In caso affermativo, l'organismo notificato ne informa il fabbricante.

   Il fabbricante informa l'organismo notificato che detiene la documentazione tecnica relativa al certificato di esame UE del tipo di tutte le modifiche al tipo omologato e ai processi di gestione delle vulnerabilità che possono influire sulla conformità ai requisiti essenziali di cui all'allegato I o sulle condizioni di validità del certificato. Tali modifiche comportano una nuova approvazione, sotto forma di un supplemento al certificato originario di esame UE del tipo.

8. Ogni organismo notificato informa le proprie autorità di notifica dei certificati di esame UE del tipo e/o dei relativi supplementi da esso rilasciati o ritirati e mette a disposizione di tali autorità, periodicamente o su richiesta, l'elenco dei certificati e/o dei relativi supplementi respinti, sospesi o altrimenti sottoposti a restrizioni.

   Ogni organismo notificato informa gli altri organismi notificati in merito ai certificati di esame UE del tipo e/o agli eventuali supplementi da esso rifiutati, ritirati, sospesi o altrimenti sottoposti a restrizioni e, su richiesta, in merito ai certificati e/o agli eventuali supplementi da esso rilasciati.

   La Commissione, gli Stati membri e gli altri organismi notificati possono ottenere, su richiesta, copia dei certificati di esame UE del tipo e/o dei relativi supplementi. La Commissione e gli Stati membri possono ottenere, su richiesta, copia della documentazione tecnica e dei risultati degli esami effettuati dall'organismo notificato. L'organismo notificato conserva una copia del certificato di esame UE del tipo e dei relativi allegati e supplementi, nonché il fascicolo tecnico contenente la

documentazione presentata dal fabbricante, fino alla scadenza della validità del certificato.

9. Il fabbricante tiene a disposizione delle autorità nazionali una copia del certificato di esame UE del tipo e dei relativi allegati e supplementi insieme alla documentazione tecnica per dieci anni dalla data in cui il prodotto è stato immesso sul mercato ***o per il periodo di supporto***.

10. Il rappresentante autorizzato del fabbricante può presentare la domanda di cui al punto 3 e ottemperare agli obblighi di cui ai punti 7 e 9, purché siano specificati nel mandato.

Conformità al tipo basata sul controllo interno della produzione (basata sul modulo C)

1. La conformità al tipo basata sul controllo interno della produzione è la parte di una procedura di valutazione della conformità con cui il fabbricante ottempera agli obblighi di cui ai punti 2 e 3 e si accerta e dichiara che i prodotti interessati sono conformi al tipo descritto nel certificato di esame UE del tipo e soddisfano i requisiti essenziali di cui all'allegato I, sezione 1.

2. Produzione

2.1. Il fabbricante adotta tutte le misure necessarie affinché il processo di produzione e il suo controllo garantiscano la conformità dei prodotti fabbricati al tipo omologato descritto nel certificato di esame UE del tipo e ai requisiti essenziali di cui all'allegato I, sezione 1.

3. Marcatura di conformità e dichiarazione di conformità

3.1. Il fabbricante appone la marcatura CE a ogni singolo prodotto conforme al tipo descritto nel certificato di esame UE del tipo e ai requisiti dello strumento legislativo ad esso applicabili.

3.2. Il fabbricante compila una dichiarazione scritta di conformità per un modello di prodotto e la tiene a disposizione delle autorità nazionali per dieci anni dalla data in cui il prodotto è stato immesso sul mercato ***o per il periodo di supporto***. La dichiarazione di conformità identifica il modello di prodotto per cui è stata compilata. Una copia di tale dichiarazione è messa a disposizione delle autorità competenti su richiesta.

4. Rappresentante autorizzato

Gli obblighi del fabbricante di cui al punto 3 possono essere adempiuti dal suo rappresentante autorizzato, a nome del fabbricante e sotto la sua responsabilità, purché siano specificati nel mandato.

Conformità basata sulla garanzia della qualità totale (basata sul modulo H)

1. La conformità basata sulla garanzia della qualità totale è la procedura di valutazione della conformità con cui il fabbricante ottempera agli obblighi di cui ai punti 2 e 5 e garantisce e dichiara, sotto la sua esclusiva responsabilità, che i prodotti (o le categorie di prodotti) interessati soddisfano i requisiti essenziali di cui all'allegato I, sezione 1, e che i processi di gestione delle vulnerabilità messi in atto dal fabbricante soddisfano i requisiti di cui all'allegato I, sezione 2.

2. Progettazione, sviluppo, produzione e gestione delle vulnerabilità dei prodotti con elementi digitali

Il fabbricante applica un sistema qualità approvato, come specificato al punto 3, per la progettazione, lo sviluppo e la produzione dei prodotti interessati e per la gestione delle vulnerabilità, ne mantiene l'efficacia nel corso di tutto il ciclo di vita dei prodotti in questione ed è assoggettato alla sorveglianza di cui al punto 4.

3. Sistema qualità

3.1. Il fabbricante presenta una domanda per la valutazione del suo sistema qualità per i prodotti interessati all'organismo notificato di sua scelta.

La domanda contiene:

– il nome e l'indirizzo del fabbricante e, qualora la domanda sia presentata dal suo rappresentante autorizzato, il nome e l'indirizzo di quest'ultimo;

– la documentazione tecnica per un modello di ciascuna categoria di prodotti che intende fabbricare o sviluppare. La documentazione tecnica contiene, laddove applicabile, almeno gli elementi di cui all'allegato V;

– la documentazione relativa al sistema qualità; nonché

– una dichiarazione scritta in cui si precisa che la stessa domanda non è stata presentata a nessun altro organismo notificato.

3.2. Il sistema qualità garantisce la conformità dei prodotti ai requisiti essenziali di cui all'allegato I, sezione 1, e la conformità dei processi di gestione delle vulnerabilità messi in atto dal fabbricante ai requisiti di cui all'allegato I, sezione 2.

Tutti i criteri, i requisiti e le disposizioni adottati dal fabbricante sono documentati in modo sistematico e ordinato sotto forma di misure, procedure e istruzioni scritte. Tale documentazione relativa al sistema qualità consente un'interpretazione uniforme di programmi, schemi, manuali e registri riguardanti la qualità.

Essa include in particolare un'adeguata descrizione:

– degli obiettivi di qualità e della struttura organizzativa, delle responsabilità e dei poteri del personale direttivo in materia di progettazione, sviluppo, qualità del prodotto e gestione delle vulnerabilità;

– delle specifiche di progettazione tecnica e di sviluppo, comprese le norme, che saranno applicate e, qualora non siano applicate integralmente le norme armonizzate e/o le specifiche tecniche pertinenti, degli strumenti che saranno utilizzati per garantire l'osservanza dei requisiti essenziali di cui all'allegato I, sezione 1, che si applicano ai prodotti;

– delle specifiche procedurali, comprese le norme, che saranno applicate e, qualora non siano applicate integralmente le norme armonizzate e/o le specifiche tecniche pertinenti, degli strumenti che saranno utilizzati per garantire l'osservanza dei requisiti essenziali di cui all'allegato I, sezione 2, che si applicano al fabbricante;

– delle tecniche, dei processi e degli interventi sistematici in materia di controllo e verifica della progettazione e dello sviluppo che saranno applicati nella progettazione e nello sviluppo dei prodotti appartenenti alla categoria di prodotti in questione;

– delle tecniche, dei processi e degli interventi sistematici che saranno applicati nella produzione, nel controllo di qualità e nella garanzia della qualità;

– degli esami e delle prove che saranno effettuati prima, durante e dopo la produzione, con indicazione della frequenza con cui si intende effettuarli;

– della documentazione in materia di qualità, quali le relazioni sulle ispezioni e i dati relativi alle prove e alle tarature, i rapporti sulle qualifiche del personale interessato ecc.;

– dei mezzi di controllo delle modalità per ottenere la qualità di progettazione e la qualità del prodotto richieste e dell'efficace funzionamento del sistema qualità.

3.3. L'organismo notificato valuta il sistema qualità per determinare se soddisfa i requisiti di cui al punto 3.2.

L'organismo presume la conformità a tali requisiti degli elementi del sistema qualità conformi alle specifiche corrispondenti della norma nazionale che attua la norma armonizzata e/o la specifica tecnica pertinente.

Oltre ad avere esperienza nei sistemi di gestione della qualità, almeno un membro del gruppo incaricato dell'audit ha esperienza nella valutazione del settore e della tecnologia del prodotto in questione e conosce i requisiti applicabili del presente regolamento. L'audit prevede una visita di valutazione dei locali del fabbricante, ove esistenti. Il gruppo incaricato dell'audit esamina la documentazione tecnica di cui al punto 3.1, secondo trattino, per verificare la capacità del fabbricante di individuare i requisiti applicabili del presente regolamento e di effettuare gli esami necessari atti a garantire la conformità del prodotto a tali requisiti.

La decisione è notificata al fabbricante o al suo rappresentante autorizzato.

La notifica contiene le conclusioni dell'audit e la motivazione circostanziata della decisione.

3.4. Il fabbricante si impegna a soddisfare gli obblighi derivanti dal sistema qualità approvato e a fare in modo che esso rimanga adeguato ed efficace.

3.5. Il fabbricante tiene informato l'organismo notificato che ha approvato il sistema qualità delle modifiche che intende apportare a tale sistema.

L'organismo notificato valuta le modifiche proposte e decide se il sistema qualità modificato continui a soddisfare i requisiti di cui al punto 3.2 o se sia necessaria una nuova verifica.

Esso notifica la decisione al fabbricante. La notifica contiene le conclusioni dell'esame e la motivazione circostanziata della decisione.

4. Sorveglianza sotto la responsabilità dell'organismo notificato

4.1. Scopo della sorveglianza è garantire che il fabbricante ottemperi debitamente agli obblighi derivanti dal sistema qualità approvato.

4.2. Il fabbricante consente all'organismo notificato di accedere, ai fini della valutazione, ai locali di progettazione, sviluppo, produzione, ispezione, prova e deposito fornendo tutte le necessarie informazioni, in particolare:

– la documentazione relativa al sistema qualità;

– la documentazione in materia di qualità prevista nella sezione del sistema qualità riservata alla progettazione, come i risultati di analisi, calcoli, prove ecc.;

– la documentazione in materia di qualità prevista nella sezione del sistema qualità relativa alla fabbricazione, come le relazioni sulle ispezioni e i dati relativi alle prove e alle tarature, i rapporti sulle qualifiche del personale interessato ecc.

4.3. L'organismo notificato svolge audit periodici intesi ad accertare che il fabbricante mantenga e applichi il sistema qualità e fornisce al fabbricante una relazione sugli audit effettuati.

5. Marcatura di conformità e dichiarazione di conformità

5.1. Il fabbricante appone la marcatura CE e, sotto la responsabilità dell'organismo notificato di cui al punto 3.1, il numero di identificazione di quest'ultimo, su ogni singolo prodotto che soddisfa i requisiti di cui all'allegato I, sezione 1, del presente regolamento.

5.2. Il fabbricante compila una dichiarazione di conformità per ciascun modello di prodotto e la tiene a disposizione delle autorità nazionali per un periodo di dieci anni dalla data in cui il prodotto è stato immesso sul mercato ***o per il periodo di supporto***. La dichiarazione di conformità identifica il modello di prodotto per cui è stata compilata.

Una copia di tale dichiarazione è messa a disposizione delle autorità competenti su richiesta.

6. Il fabbricante, per almeno dieci anni dalla data in cui il prodotto è stato immesso sul mercato ***o per il periodo di supporto o per il periodo durante il quale sono trattate le vulnerabilità***, tiene a disposizione delle autorità nazionali.

– la documentazione tecnica di cui al punto 3.1;

– la documentazione relativa al sistema qualità di cui al punto 3.1;

– le modifiche di cui al punto 3.5 e la relativa approvazione;

– le decisioni e le relazioni trasmesse dall'organismo notificato di cui ai punti 3.5, 4.3 e 4.4.

7. Ogni organismo notificato informa le proprie autorità di notifica delle approvazioni dei sistemi qualità rilasciate o ritirate e, periodicamente o su richiesta, mette a loro disposizione l'elenco delle approvazioni dei sistemi qualità respinte, sospese o altrimenti sottoposte a restrizioni.

Ogni organismo notificato informa gli altri organismi notificati delle approvazioni dei sistemi qualità da esso rifiutate, sospese o ritirate e, a richiesta, delle approvazioni dei sistemi qualità rilasciate.

8. Rappresentante autorizzato

Gli obblighi del fabbricante di cui ai punti 3.1, 3.5, 5 e 6 possono essere adempiuti dal suo rappresentante autorizzato, a nome del fabbricante e sotto la sua responsabilità, purché siano specificati nel mandato.

ALLEGATO VI bis

ESIGENZE DI CAPACITÀ DELL'AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA (ENISA)

Per adempiere ai suoi obblighi a norma del presente regolamento e per non compromettere gli obblighi esistenti dell'Agenzia a norma di altra legislazione dell'Unione, all'ENISA sono garantiti personale e finanziamenti adeguati. Pertanto, i compiti aggiuntivi per l'ENISA a norma del presente regolamento sono accompagnati da risorse umane e finanziarie supplementari. Per coprire i compiti supplementari previsti dal presente regolamento saranno necessari nove posti supplementari equivalenti a tempo pieno e i corrispondenti stanziamenti supplementari.

MOTIVAZIONE

Il relatore accoglie con grande favore la proposta della Commissione di affrontare le carenze di cibersicurezza nei prodotti hardware e software. Nel 2021 il costo globale della criminalità informatica ha raggiunto i 5,5 miliardi di EUR. Questo fenomeno, associato alla tendenza all'aumento della digitalizzazione, richiede che legislatori garantiscano la messa in atto misure di cibersicurezza adeguate per tutelare gli interessi sia dei consumatori che dell'industria.

In questo contesto il relatore è lieto che la Commissione abbia presentato una proposta ambiziosa, che potenzierà il livello generale di cibersicurezza negli Stati membri e il funzionamento del mercato interno. Un quadro normativo armonizzato è necessario affinché le imprese che operano nel mercato unico possano beneficiare di chiarezza giuridica, nonché per garantire che l'Unione possa svolgere un ruolo guida nella definizione di norme in materia di cibersicurezza sulla scena mondiale.

Per quanto riguarda l'ambito di applicazione, il relatore concorda con la proposta della Commissione di includere tutti i prodotti con elementi digitali. Tale approccio globale garantirebbe la conformità della cibersicurezza lungo tutta la catena del valore, migliorando la competitività e l'attrattiva dei prodotti fabbricati nell'Unione. È tuttavia necessario semplificare l'attuale formulazione e fare riferimento ai prodotti direttamente e indirettamente collegabili, escludendo nel contempo i pezzi di ricambio progettati esclusivamente per il processo di riparazione che erano presenti sul mercato prima dell'entrata in vigore del regolamento in esame Per quanto riguarda il software open source, il relatore è consapevole della necessità di salvaguardare questa importante fonte di innovazione e ha pertanto presentato un emendamento volto a garantire che gli sviluppatori non siano tenuti a rispettare il presente regolamento se non ricevono alcun rendimento finanziario per i loro progetti. Tuttavia, è opportuno includere il software open source fornito nel quadro di un'attività commerciale, al fine di garantire la cibersicurezza dell'ecosistema dell'Unione.

Mentre la stragrande maggioranza dei prodotti con elementi digitali dovrà essere sottoposta solo all'autovalutazione, i prodotti critici a norma dell'articolo 6 saranno sottoposti a valutazione da parte di terzi. A tale proposito il relatore ritiene che il regolamento dovrebbe essere migliorato fornendo maggiore chiarezza sulla frequenza con cui è possibile modificare l'elenco di cui all'allegato III e sulle procedure da seguire dopo l'aggiunta di un prodotto all'elenco. Quest'ultimo aspetto è particolarmente importante per dare alle imprese il tempo necessario per adeguarsi. Tuttavia, il relatore ritiene che i sistemi domotici e i prodotti che migliorano la sicurezza privata, come le telecamere e le serrature intelligenti, dovrebbero costituire prodotti critici di classe I. Ciò è dovuto al fatto che l'integrità di tali beni è fondamentale per la sicurezza e la vita privata dei cittadini.

Inoltre, il progetto di relazione prevede un maggiore coinvolgimento dei portatori di interessi attraverso la creazione del gruppo di esperti sulla ciberresilienza. Tale organismo dovrebbe essere incaricato di fornire consulenza alla Commissione e di svolgere un ruolo attivo nella preparazione degli atti delegati di cui al presente regolamento. Pertanto, al fine di esprimere pienamente gli interessi di tutte le parti, il gruppo di esperti dovrebbe essere composto da istituzioni, industria, società civile, mondo accademico e singoli esperti.

Oltre all'argomento summenzionato, il progetto di relazione sottolinea la necessità che gli

Stati membri tengano fortemente conto della cibersicurezza negli appalti pubblici di prodotti con elementi digitali e garantiscano che le vulnerabilità siano affrontate tempestivamente. Per quanto riguarda gli obblighi dei fabbricanti, il relatore ritiene che una data fissa per la durata di vita prevista del prodotto non sia adeguata nel caso di un regolamento orizzontale, che intende coprire un'ampia gamma di prodotti, dai software ai telefoni e ai macchinari industriali. Per questo motivo il relatore ritiene che sia più opportuno che i fabbricanti determinino la durata di vita dei loro rispettivi prodotti, a condizione che la durata proposta sia compatibile con le ragionevoli aspettative dei consumatori. Una durata flessibile consentirebbe inoltre ai fabbricanti di mettere in mostra i loro prodotti e di avere una lunga durata di vita come elemento di competitività. Pertanto, al fine di sensibilizzare i consumatori a questa particolare questione, il regolamento dovrebbe anche obbligare i fabbricanti a indicare chiaramente la durata di vita prevista del prodotto sull'imballaggio o a includerla negli accordi contrattuali, e a informare i consumatori quando il ciclo di vita è in procinto di concludersi. Inoltre, il progetto di relazione intende porre la massima enfasi sulla sicurezza. Pertanto, il relatore ritiene che i fabbricanti dovrebbero anche essere obbligati ad aggiornare automaticamente, ove possibile, le caratteristiche di sicurezza dei rispettivi prodotti. Se un fabbricante ha definito una durata di vita prevista inferiore a cinque anni, dovrebbe essere pronto a concludere accordi contrattuali con le imprese che desiderano fornire servizi che prolungano la durata di vita di un prodotto e a comunicare loro il suo codice sorgente. Tale possibilità non dovrebbe comportare un trasferimento di proprietà o la divulgazione al pubblico del codice sorgente.

Per quanto riguarda gli obblighi di comunicazione a norma dell'articolo 11, il relatore desidera allineare il calendario alla direttiva NIS2 in modo da garantire maggiore coerenza e certezza giuridica per le parti interessate. In tal senso, il relatore suggerisce di segnalare incidenti significativi (piuttosto che tutti gli incidenti), nonché vulnerabilità attivamente sfruttate, a condizione che siano in vigore protocolli chiari su come gestire tali notifiche in modo sicuro, in modo da evitare la diffusione di informazioni sulle vulnerabilità non risolte. Il relatore introduce inoltre un meccanismo di segnalazione volontaria per altri incidenti, quasi incidenti e minacce informatiche.

Tuttavia, per massimizzare l'effetto della comunicazione è importante disporre di un'entità unica, anche al fine di semplificare gli obblighi di comunicazione per i costruttori in tutta l'Unione. A tale proposito, il relatore ritiene che l'organismo migliore per svolgere questo ruolo sia l'ENISA. Pertanto, alla luce dell'aumento dei compiti e delle competenze assegnati all'ENISA, la Commissione dovrebbe modificare la scheda finanziaria legislativa che accompagna il presente regolamento fornendo all'Agenzia dell'Unione europea per la cibersicurezza posti supplementari e corrispondenti stanziamenti supplementari al fine di svolgere i compiti aggiuntivi dell'agenzia di cui al presente regolamento.

Inoltre, una questione fondamentale per il relatore è garantire un sostegno sufficiente affinché le imprese attuino i requisiti del presente regolamento. Ciò vale in particolare per le microimprese e le piccole e medie imprese, che, date le loro capacità limitate, possono incontrare difficoltà nel garantire il rispetto della legge sulla ciberresilienza. Il relatore ritiene pertanto essenziale estendere a 40 mesi la data di applicazione del regolamento. In tale periodo transitorio per i fabbricanti dovrebbe essere possibile ottemperare alla legge sulla ciberresilienza su base volontaria, al fine di ottenere una presunzione di conformità con il regolamento delegato sulla direttiva sulle apparecchiature radio e di adeguarsi al presente regolamento prima della sua attuazione ufficiale. Inoltre, il relatore desidera sottolineare

l'importanza che l'Unione fornisca sostegno per il miglioramento delle competenze e la riqualificazione dei lavoratori e garantisca la disponibilità di professionisti della cibersicurezza, un elemento chiave per il successo del regolamento in esame.

Inoltre, come approccio generale per aiutare tutti i portatori di interessi, il relatore chiede alla Commissione di definire orientamenti più precisi sull'effettiva fase di attuazione, fornendo in tal modo maggiore chiarezza a tutte le parti coinvolte.

Un'altra questione altrettanto pressante per il relatore è il commercio internazionale. Per questo motivo il progetto di relazione invita la Commissione a prendere in considerazione accordi di riconoscimento reciproco con paesi terzi affini, laddove questi condividano un livello comparabile di sviluppo tecnico e abbiano un approccio compatibile in materia di valutazione della conformità, garantendo lo stesso livello di protezione previsto dal regolamento in esame Tuttavia, è essenziale garantire un adeguato monitoraggio dei prodotti provenienti da paesi a rischio, che possono contenere backdoor o altre vulnerabilità: l'ENISA dovrebbe coordinarsi con le autorità di vigilanza del mercato ed effettuare i necessari controlli sui venditori che potrebbero presentare un profilo di rischio più elevato.

Infine, il relatore ritiene che le entrate generate dalle sanzioni dovrebbero essere destinate a progetti tesi ad aumentare il livello generale di cibersicurezza in tutta l'Unione e, di conseguenza, al programma Europa digitale, sostenendo progetti che mirano, tra l'altro, alla riqualificazione e al miglioramento delle competenze della forza lavoro attuale.

ALLEGATO: ELENCO DELLE ENTITÀ O DELLE PERSONE DA CUI IL RELATORE PER PARERE HA RICEVUTO CONTRIBUTI

L'elenco in appresso è compilato su base puramente volontaria, sotto l'esclusiva responsabilità del relatore. Nel corso dell'elaborazione della relazione, fino alla sua approvazione in commissione, il relatore ha ricevuto contributi dalle seguenti entità o persone:

Entità e/o persona
(ISC)2
ACEM
Airlines4Europe
Alliance for IoT and Edge Computing Innovation
Amazon
American Chamber of Commerce
ANEC
Apple
APPLiA
Associazione Italiana Internet Provider
BDI
Beuc
Bitkom
BritCham
Broadcom
BSA - The Software alliance
Business Europe
Card Payment Sweden
CEMA
Centrum für Europäische Politik
CNH
Confederation of Danish Industries (DI)
Confindustria
Cybersecurity Coalition
DEKRA
Deutsche Telekom
Developers Alliance
Digital Europe
Enedis
Engineering
Ericsson
ESMIG
ETNO
ETRMA
European Cybersecurity Organisation
European Materials Handling Federation (FEM)
Eurosmart

Federunacoma
Free Software Foundation Europe
German Insurance Association
Giesecke+Devrient
GitHub
Google
GSMA
Hanbury Strategy
Huawei
IBM
Independent Retail Europe
Information Technology Industry Council
Leaseurope
Lenovo
Mechanical Engineering Industry Association (VDMA)
MedTechEurope
Microsoft
Okta
Open Forum Europe
Orange
Orgalim
Permanent Representation of Belgium
Permanent Representation of Italy
Permanent Representation of the Netherlands
Piaggio
Privacy International
SAP
Schneider Electric
Siemens
SME United
Splunk
Technology Industries of Finland
Telefonica
TIC Council
Trellix
Twillio
Unife
Vodafone Group
Wikimedia
Worldr
Xiaomi
Zoom

30.6.2023

PARERE DELLA COMMISSIONE PER IL MERCATO INTERNO E LA PROTEZIONE DEI CONSUMATORI

destinato alla commissione per l'industria, la ricerca e l'energia

sulla 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
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Relatore per parere (*): Morten Løkkegaard

(*) Procedura con le commissioni associate – articolo 57 del regolamento

BREVE MOTIVAZIONE

In qualità di ex relatore per parere nella commissione IMCO sulla direttiva NIS2, il relatore ritiene che la legge sulla ciberresilienza rappresenti il naturale passo successivo, di importanza cruciale, per migliorare la cibersicurezza dell'Unione europea. Consapevole del fatto che, per definizione, la cibersicurezza non sarà mai completa al 100 %, il relatore è del parere che sia importante fare tutto ciò che è in nostro potere per ridurre il numero di anelli deboli nella nostra Unione, e per questo motivo la legge sulla ciberresilienza è accolta come un passo successivo apprezzato. È necessario aumentare la cibersicurezza dei prodotti con elementi digitali e altri nuovi prodotti come i dispositivi IoT, che sono diventati parte integrante della vita quotidiana delle imprese e dei consumatori europei.

Poiché la commissione IMCO è responsabile del funzionamento e dell'attuazione del mercato unico, compreso il mercato unico digitale, e delle norme sulla protezione dei consumatori, il relatore ha cercato di introdurre emendamenti volti a migliorare il funzionamento del mercato interno, prevedendo nel contempo un'elevato livello di protezione dei consumatori nell'ambito della proposta, in particolare per quanto riguarda i requisiti di cibersicurezza per i prodotti con elementi digitali.

Inoltre, il relatore ritiene che taluni aspetti del regolamento proposto richiedano un miglioramento al fine di garantire certezza giuridica e coerenza tra le disposizioni pertinenti del regolamento proposto e gli altri atti legislativi. Ciò riguarda in particolare la direttiva NIS2, il regolamento relativo alla sicurezza generale dei prodotti recentemente adottato, il regolamento sull'intelligenza artificiale e il regolamento sulle macchine, nonché una serie di atti delegati e atti di esecuzione pertinenti. Pertanto, il relatore ha proposto emendamenti volti a migliorare la chiarezza giuridica e contribuire a garantire un'interpretazione e un'applicazione coerenti, efficaci e uniformi delle normative citate.

Inoltre, poiché le micro, piccole e medie imprese sono operatori economici cruciali nel mercato digitale, il relatore ha introdotto una serie di emendamenti per semplificare le procedure amministrative e limitare l'onere amministrativo per le piccole imprese, senza abbassare il

livello di sicurezza. Inoltre, il relatore ha introdotto emendamenti che assicurano che le microimprese e le PMI ricevano orientamenti e consigli specifici per adempiere ai requisiti della legge sulla ciberresilienza.

Infine, il relatore ha introdotto emendamenti finalizzati a garantire una comunicazione più efficace con le autorità competenti (autorità nazionali di vigilanza del mercato, ENISA), nonché a rafforzare le disposizioni relative agli obblighi e alle competenze delle autorità competenti in materia di reclami, ispezioni e attività congiunte. Inoltre, alcuni emendamenti del relatore si concentrano sul miglioramento dei requisiti di cibersicurezza per i componenti integrati nei prodotti finali con elementi digitali, specificando gli obblighi degli operatori economici, come i fabbricanti e i rappresentanti autorizzati.

Il relatore ribadisce la posizione secondo cui l'introduzione della legge sulla ciberresilienza è il passo successivo, naturale e opportuno, per rafforzare la rete intorno alle minacce alla cibersicurezza nella nostra Unione. Con gli emendamenti suggeriti, il relatore ha cercato di trovare il giusto equilibrio tra la garanzia di un maggiore livello di cibersicurezza a vantaggio dei consumatori europei e un onere proporzionato per la comunità imprenditoriale. L'ambizione del relatore è che la cibersicurezza diventi un parametro naturale della concorrenza nel mercato interno. È in quest'ottica che il relatore ha cercato di adeguare la proposta

EMENDAMENTI

La commissione per il mercato interno e la protezione dei consumatori invita la commissione per l'industria, la ricerca e l'energia, competente per il merito, a prendere in considerazione i seguenti emendamenti:

Emendamento 1

Proposta di regolamento
Considerando 1

Testo della Commissione	*Emendamento*
(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.	(1) Occorre migliorare il funzionamento del mercato interno ***e garantire al tempo stesso un livello elevato di protezione dei consumatori e di cibersicurezza,*** 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.

Emendamento 2

Proposta di regolamento
Considerando 7

Testo della Commissione	*Emendamento*
(7) In determinate condizioni tutti i prodotti con elementi digitali integrati in un sistema di informazione elettronico più	(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 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.	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 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 ***connessi a una rete o un dispositivo esterni*** siano progettati e sviluppati conformemente ai requisiti essenziali stabiliti nel presente regolamento. Sono compresi sia i prodotti che possono essere connessi ***a reti o dispositivi esterni*** 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.

Emendamento 3

Proposta di regolamento
Considerando 7 bis (nuovo)

Testo della Commissione	*Emendamento*
	(7 bis) Il presente regolamento non dovrebbe applicarsi alle reti interne di un prodotto con elementi digitali laddove tali reti siano dotate di endpoint dedicati e siano completamente isolate e protette da una connessione dati esterna.

Emendamento 4

Proposta di regolamento
Considerando 7 ter (nuovo)

Testo della Commissione	*Emendamento*
	(7 ter) Il presente regolamento non dovrebbe applicarsi alle parti di ricambio destinate esclusivamente a sostituire parti difettose di prodotti con elementi digitali, al fine di ripristinarne la funzionalità.

Emendamento 5

Proposta di regolamento
Considerando 9

Testo della Commissione	*Emendamento*
(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.	(9) Il presente regolamento garantisce un livello elevato di cibersicurezza dei prodotti con elementi digitali. Esso non disciplina servizi come il servizio a livello di software (Software-as-a-Service – SaaS). 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.

Emendamento 6

Proposta di regolamento
Considerando 10

Testo della Commissione	*Emendamento*
(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.	(10) ***I software e i dati che sono condivisi apertamente e che gli utenti possono liberamente consultare, utilizzare, modificare e ridistribuire, comprese le loro versioni modificate, possono contribuire alla ricerca e all'innovazione nel mercato. Dalle ricerche condotte dalla Commissione emerge anche che i software liberi e open source possono contribuire al PIL dell'Unione per un valore compreso tra i 65 e i 95 miliardi di EUR e offrire notevoli opportunità di crescita per l'economia europea.*** 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. Un'attività commerciale***, nel senso di una messa a disposizione sul mercato,*** può ***tuttavia*** essere caratterizzata dall'applicazione di un prezzo per un ***componente software libero e open source***, ma anche ***da una monetizzazione come l'applicazione*** di un prezzo per i servizi di assistenza tecnica, ***o aggiornamenti del software a pagamento, salvo laddove ciò non sia finalizzato esclusivamente a recuperare i costi effettivi,*** 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. ***Né lo sviluppo collaborativo di***

	componenti software liberi e open source né la loro messa a disposizione su archivi aperti dovrebbero essere considerati un'immissione sul mercato o una messa in servizio. Le circostanze in cui il prodotto è stato sviluppato o il modo in cui lo sviluppo è stato finanziato non dovrebbero essere presi in considerazione al fine di determinare la natura commerciale o non commerciale di tale attività. Se un software open source è integrato in un prodotto finale con elementi digitali immesso sul mercato, l'operatore economico che ha immesso sul mercato il prodotto finale con elementi digitali dovrebbe essere responsabile della conformità del prodotto, ivi incluso dei componenti liberi e open source.

Emendamento 7

Proposta di regolamento
Considerando 11

Testo della Commissione	*Emendamento*
(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	(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 ***connessi a una rete o un dispositivo esterni***, mira anche a facilitare il rispetto dei requisiti relativi alla catena di approvvigionamento

[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.

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.

Emendamento 8

Proposta di regolamento
Considerando 15

Testo della Commissione	*Emendamento*
(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 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	(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, ***quando*** la Commissione abroga il 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

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.	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.

Emendamento 9

Proposta di regolamento
Considerando 18 bis (nuovo)

Testo della Commissione	*Emendamento*
	(18 bis) Al fine di garantire che i singoli o i micro sviluppatori di software, quali definiti nella raccomandazione 2003/361/CE della Commissione, non debbano affrontare ingenti oneri finanziari e non siano scoraggiati dal testare la dimostrazione di concetto e la giustificazione economica sul mercato, è opportuno che tali soggetti siano tenuti ad adoperarsi al meglio per conformarsi ai requisiti di cui alla presente proposta nei sei mesi successivi all'immissione di un software sul mercato. Tale regime speciale dovrebbe evitare l'effetto dissuasivo che gli elevati costi di conformità e di immissione potrebbero avere sugli imprenditori o sulle persone qualificate che intendano sviluppare software nell'Unione. Tuttavia, tale regime speciale non dovrebbe applicarsi ai prodotti altamente critici con elementi digitali.

Emendamento 10

Proposta di regolamento
Considerando 19

Testo della Commissione	*Emendamento*
(19) Alcuni compiti previsti dal presente	(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

regolamento dovrebbero essere svolti dall'ENISA, conformemente all'articolo 3, paragrafo 2, del regolamento (UE) 2019/881. In particolare l'ENISA dovrebbe ricevere***, mediante una segnalazione preventiva,*** le notifiche dei fabbricanti relative alle vulnerabilità attivamente sfruttate contenute nei prodotti con elementi digitali, nonché agli incidenti che hanno un impatto ***significativo*** 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 ***immediatamente*** le autorità di vigilanza del mercato competenti in merito ***all'esistenza di una*** vulnerabilità ***e, se del caso, alle misure di attenuazione dei rischi potenziali***. ***Qualora a una vulnerabilità notificata non corrispondano misure correttive o di attenuazione, l'ENISA dovrebbe garantire che le informazioni sulla vulnerabilità notificata siano condivise in conformità di rigorosi protocolli di sicurezza e in base al principio della necessità di sapere.*** 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

funzionamento del mercato interno.	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.

Emendamento 11

Proposta di regolamento
Considerando 20

Testo della Commissione	*Emendamento*
(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.	(20) I prodotti con elementi digitali dovrebbero recare la marcatura CE per indicare ***in modo visibile, leggibile e indelebile*** 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.

Emendamento 12

Proposta di regolamento
Considerando 22

Testo della Commissione	*Emendamento*
(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	(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.	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***, come adeguamenti di modesta entità del codice sorgente che ne possono migliorare la sicurezza e il funzionamento,*** 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.

Emendamento 13

Proposta di regolamento
Considerando 23

Testo della Commissione	*Emendamento*
(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	(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, se del caso, ***aggiornarne la*** 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.	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. ***La valutazione della conformità aggiornata dovrebbe riguardare le modifiche che hanno condotto alla nuova valutazione, a meno che tali modifiche non abbiano un impatto significativo sulla conformità di altre parti del prodotto. Se il software è aggiornato, il fabbricante non dovrebbe essere tenuto a effettuare un'altra valutazione di conformità del prodotto con elementi digitali, a meno che l'aggiornamento del software non comporti una modifica sostanziale del prodotto con elementi digitali.***

Emendamento 14

Proposta di regolamento
Considerando 24 bis (nuovo)

Testo della Commissione	*Emendamento*
	(24 bis) I fabbricanti di prodotti con elementi digitali dovrebbero garantire che gli aggiornamenti del software siano forniti in modo chiaro e trasparente e operare una chiara distinzione tra aggiornamenti di sicurezza e aggiornamenti delle funzionalità. Mentre gli aggiornamenti di sicurezza sono progettati per ridurre il livello di rischio di un prodotto con elementi digitali, l'installazione degli aggiornamenti delle funzionalità forniti dal fabbricante dovrebbe sempre essere a discrezione dell'utente. I fabbricanti dovrebbero quindi fornire tali aggiornamenti separatamente, salvo se tecnicamente impossibile. I fabbricanti dovrebbero fornire ai consumatori informazioni adeguate sui motivi di ciascun aggiornamento e sul suo impatto previsto sul prodotto, nonché un meccanismo di

non partecipazione chiaro e di facile utilizzo.

Emendamento 15

Proposta di regolamento
Considerando 25

Testo della Commissione	*Emendamento*
(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.	(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, ***in applicazioni critiche in ambienti sensibili*** 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.

Emendamento 16

Proposta di regolamento
Considerando 26

Testo della Commissione	*Emendamento*
(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	(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.	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. ***In via eccezionale, le piccole e micro imprese dovrebbero avere la possibilità di ricorrere alla procedura per i prodotti di classe I.***

Emendamento 17

Proposta di regolamento
Considerando 29

Testo della Commissione	*Emendamento*
(29) I prodotti con elementi digitali classificati come sistemi di IA ad alto rischio conformemente all'articolo 6 del regolamento[27] [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 contemplato dal presente regolamento e classificato come sistema di IA ad alto rischio, è opportuno	(29) I prodotti con elementi digitali ***o i prodotti parzialmente completati con elementi digitali*** classificati come sistemi di IA ad alto rischio conformemente all'articolo 6 del regolamento[27] [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 contemplato dal

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]***.	presente regolamento e classificato come sistema di IA ad alto rischio, è opportuno che si applichino come norma generale le disposizioni pertinenti ***[delle disposizioni applicabili]*** del regolamento [regolamento sull'IA] anziché le rispettive disposizioni del presente regolamento. Tale norma dovrebbe ***creare un elevato*** livello di garanzia necessario per i prodotti con elementi digitali critici contemplati dal presente regolamento. ***Per*** 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, ***l'organismo settoriale notificato responsabile dovrebbe essere incaricato di effettuare la*** valutazione della conformità ***ai sensi*** del ***presente*** regolamento ***e guidare la procedura amministrativa in modo che gli operatori economici possano presentare la loro richiesta*** di valutazione della conformità ***a un unico organismo di regolamentazione***.
[27] Regolamento [regolamento sull'IA].	[27] Regolamento [regolamento sull'IA].

Emendamento 18

Proposta di regolamento
Considerando 32

Testo della Commissione	*Emendamento*
(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	(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.	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 adeguate.

Emendamento 19

Proposta di regolamento
Considerando 33 bis (nuovo)

Testo della Commissione	*Emendamento*
	(33 bis) Al fine di garantire che i prodotti siano progettati, sviluppati e fabbricati in linea con i requisiti essenziali previsti nell'allegato I, sezione 1, i fabbricanti dovrebbero esercitare la dovuta diligenza quando integrano componenti provenienti da terzi in prodotti con elementi digitali. Ciò si applica ai componenti che sono adattati e integrati tenendo conto delle specificità del prodotto, in particolare nel caso dei software liberi e open source che non sono stati immessi sul mercato in cambio di una monetizzazione finanziaria o di altro tipo.

Emendamento 20

Proposta di regolamento
Considerando 34

Testo della Commissione	*Emendamento*
(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.	(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***, senza indebito ritardo e comunque entro 48 ore dal momento in cui ne vengono a conoscenza, mediante una segnalazione preventiva,*** le vulnerabilità attivamente sfruttate***. I fabbricanti dovrebbero inoltre comunicare all'ENISA, senza indebito ritardo dal momento in cui vengono a conoscenza di una vulnerabilità attivamente sfruttata che ha un impatto significativo sulla sicurezza del prodotto con elementi digitali, maggiori dettagli sul tale vulnerabilità sfruttata. Tutte le altre vulnerabilità che non hanno un impatto significativo sulla sicurezza del prodotto con elementi digitali dovrebbero essere notificate all'ENISA una volta affrontate***. 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.

Emendamento 21

Proposta di regolamento
Considerando 34 bis (nuovo)

Testo della Commissione	*Emendamento*
	(34 bis) L'ENISA dovrebbe essere responsabile della pubblicazione e del mantenimento di una banca dati delle vulnerabilità sfruttate note. I fabbricanti dovrebbero monitorare la banca dati e notificare le vulnerabilità riscontrate nei loro prodotti.

Emendamento 22

Proposta di regolamento
Considerando 35

Testo della Commissione	*Emendamento*
(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	(35) I fabbricanti dovrebbero anche segnalare all'ENISA***, mediante una segnalazione preventiva,*** qualsiasi incidente che abbia un impatto ***significativo*** sulla sicurezza del prodotto con elementi digitali***. I fabbricanti dovrebbero inoltre comunicare all'ENISA, senza indebito ritardo e comunque entro 72 ore dal momento in cui vengono a conoscenza dell'incidente significativo relativo al prodotto con elementi digitali, maggiori dettagli sul tale incidente significativo***. 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

sui propri siti web o il contatto diretto, qualora il fabbricante sia in grado di contattare gli utilizzatori e ciò sia giustificato dai rischi.	rapidamente agli incidenti che hanno un impatto ***significativo*** sulla sicurezza dei loro prodotti con elementi digitali, i fabbricanti dovrebbero inoltre informare gli utilizzatori di tali incidenti ***ove opportuno e se è probabile che abbiano un impatto negativo su di essi*** e, se del caso, di ***qualsiasi misura di attenuazione dei rischi o misura correttiva*** che gli utilizzatori potrebbero adottare per attenuarne l'impatto ***significativo***, 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. ***Fatti salvi gli altri obblighi, i fabbricanti che individuano una vulnerabilità in un componente integrato in un prodotto con elementi digitali, ivi incluso in un componente libero e open source, dovrebbero segnalare la vulnerabilità alla persona o all'ente che si occupa della manutenzione del componente, unitamente alla misura correttiva adottata.***

Emendamento 23

Proposta di regolamento
Considerando 37 bis (nuovo)

Testo della Commissione	*Emendamento*
	(37 bis) Secondo l'accordo sugli ostacoli tecnici agli scambi dell'OMC, laddove siano necessari regolamenti tecnici ed esistano norme internazionali pertinenti, i membri dell'OMC dovrebbero utilizzare tali norme come base per i propri regolamenti tecnici. È importante evitare sovrapposizioni nel lavoro tra le organizzazioni di normazione, in quanto le norme internazionali mirano a facilitare l'armonizzazione delle norme e dei regolamenti tecnici nazionali e regionali, riducendo in tal modo gli ostacoli tecnici non tariffari al

	commercio. Dato che la sicurezza informatica è una questione globale, l'Unione dovrebbe impegnarsi per ottenere il massimo allineamento. Al fine di conseguire tale obiettivo, la richiesta di normazione per il presente regolamento, come stabilito all'articolo 10 del regolamento (UE) n. 1025/2012, dovrebbe mirare di ridurre gli ostacoli all'accettazione delle norme pubblicando i loro riferimenti nella Gazzetta ufficiale dell'UE, conformemente all'articolo 10, paragrafo 6, del suddetto regolamento.

Emendamento 24

Proposta di regolamento
Considerando 37 ter (nuovo)

Testo della Commissione	*Emendamento*
	(37 ter) In considerazione dell'ampio ambito di applicazione del presente regolamento, lo sviluppo tempestivo di norme armonizzate rappresenta un'importante sfida. Onde rafforzare al più presto la sicurezza dei prodotti con componenti digitali nel mercato dell'Unione, la Commissione dovrebbe avere la facoltà, per un periodo di tempo limitato, di dichiarare che le norme internazionali esistenti in materia di cibersicurezza dei prodotti soddisfano i requisiti del presente regolamento. Tali norme dovrebbero essere pubblicate in quanto norme che conferiscono la presunzione di conformità.

Emendamento 25

Proposta di regolamento
Considerando 38

Testo della Commissione	*Emendamento*
(38) Al fine di facilitare la valutazione della conformità ai requisiti stabiliti dal	(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[29]. Il regolamento (UE) n. 1025/2012 prevede una procedura di obiezione a norme armonizzate che non soddisfano completamente i requisiti del presente regolamento.

[29] 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).

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[29]. Il regolamento (UE) n. 1025/2012 prevede una procedura di obiezione a norme armonizzate che non soddisfano completamente i requisiti del presente regolamento. ***Il processo di normazione dovrebbe garantire una rappresentazione equilibrata degli interessi e un'effettiva partecipazione dei portatori di interessi della società civile, comprese le organizzazioni dei consumatori.***

[29] 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).

Emendamento 26

Proposta di regolamento
Considerando 41

Testo della Commissione	*Emendamento*
(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	(41) Se ***nessun riferimento a*** norme armonizzate ***che contemplano*** i requisiti ***di cui all'allegato I è stato pubblicato nella Gazzetta ufficiale dell'Unione europea conformemente al regolamento (UE)***

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.

n. 1025/2012 e non si prevede la pubblicazione di tale riferimento entro un termine ragionevole, 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.

Emendamento 27

Proposta di regolamento
Considerando 43

Testo della Commissione	*Emendamento*
(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[30]. 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	(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[30]. 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.	regolamento. ***Tuttavia, un prodotto parzialmente completato con elementi digitali non reca la marcatura CE prevista dal presente regolamento, fatte salve le disposizioni in materia di marcatura derivanti da altre normative dell'Unione applicabili. Per i prodotti parzialmente completati con elementi digitali, i fabbricanti dovrebbero redigere una dichiarazione di incorporazione UE.***
[30] 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).	[30] 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).

Emendamento 28

Proposta di regolamento
Considerando 45

Testo della Commissione	*Emendamento*
(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	(45) La valutazione ***dei requisiti di*** conformità dei prodotti con elementi digitali dovrebbe essere di norma ***basata sul rischio e, in tal senso, in molti casi potrebbe essere*** 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 o i sistemi di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881 che sono stati

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.	identificati dalla Commissione in un atto di esecuzione. Se non applica tali norme armonizzate 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.

Emendamento 29

Proposta di regolamento
Considerando 46 bis (nuovo)

Testo della Commissione	*Emendamento*
	(46 bis) In caso di equivalenza tra prodotti con elementi digitali, uno di tali prodotti può essere accettato come rappresentativo di una famiglia o categoria di prodotti ai fini di determinate procedure di valutazione della conformità.

Emendamento 30

Proposta di regolamento
Considerando 55

Testo della Commissione	*Emendamento*
(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.	(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 ***8*** della direttiva ***2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (***direttiva NIS 2) 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.

Emendamento 31

Proposta di regolamento
Considerando 56 bis (nuovo)

Testo della Commissione	*Emendamento*
	(56 bis) Affinché gli operatori economici che sono PMI e microimprese siano in grado di adempiere ai nuovi obblighi imposti dal presente regolamento, la Commissione dovrebbe fornire loro orientamenti e consigli di facile comprensione, ad esempio tramite un canale diretto per comunicare con gli esperti in caso di domande, tenendo conto della necessità di semplificare e limitare gli oneri amministrativi. Nell'elaborare tali orientamenti, la Commissione dovrebbe tenere conto delle esigenze delle PMI in modo da ridurre al minimo gli oneri amministrativi e finanziari, facilitando nel contempo la loro conformità al presente regolamento. La Commissione dovrebbe consultare i portatori di interessi pertinenti con competenze nell'ambito della cibersicurezza.

Emendamento 32

Proposta di regolamento
Considerando 58

Testo della Commissione	*Emendamento*
(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,	(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.

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 ***(UE) 2022/255*** (***direttiva*** 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.

Emendamento 33

Proposta di regolamento
Considerando 59

Testo della Commissione	*Emendamento*
(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.	(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 ***(UE) 2022/2555*** (***direttiva*** 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 ***(UE) 2022/2555*** (***direttiva*** 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.

Emendamento 34

Proposta di regolamento
Considerando 62

Testo della Commissione	*Emendamento*
(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[33]. 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 esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei	(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 certificazione ***volontaria*** 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[33]. 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 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.

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

gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

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

Emendamento 35

Proposta di regolamento
Considerando 63

Testo della Commissione	*Emendamento*
(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[34].	(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 ***sulla base delle migliori pratiche del settore***, 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[34].

[34] 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).

[34] 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).

Emendamento 36

Proposta di regolamento
Considerando 69

Testo della Commissione	*Emendamento*
(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***.	(69) Agli operatori economici dovrebbe essere concesso un periodo di tempo sufficiente per adeguarsi ai requisiti del presente regolamento. Il presente regolamento dovrebbe applicarsi [***36*** mesi] dopo la sua entrata in vigore

Emendamento 37

Proposta di regolamento
Articolo 1 – parte introduttiva

Testo della Commissione	*Emendamento*
Il presente regolamento stabilisce:	***L'obiettivo generale del presente regolamento è quello di migliorare il funzionamento del mercato interno, garantendo un livello elevato di protezione dei consumatori e di cibersicurezza.*** Il presente regolamento stabilisce ***norme armonizzate per quanto riguarda***:

Emendamento 38

Proposta di regolamento
Articolo 1 – lettera a

Testo della Commissione	*Emendamento*
a) ***norme per*** l'immissione sul mercato di prodotti con elementi digitali per garantire la cibersicurezza di tali prodotti;	a) l'immissione sul mercato di prodotti con elementi digitali per garantire la cibersicurezza di tali prodotti;

Emendamento 39

Proposta di regolamento
Articolo 1 – lettera d

Testo della Commissione	*Emendamento*
d) ***norme sulla*** vigilanza del mercato e ***sull'applicazione*** delle norme e dei requisiti di cui sopra.	d) ***la*** vigilanza del mercato e ***l'applicazione*** delle norme e dei requisiti di cui sopra.

Emendamento 40

Proposta di regolamento
Articolo 2 – paragrafo 1

Testo della Commissione	*Emendamento*
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.	1. Il presente regolamento si applica ai prodotti con elementi digitali ***immessi sul mercato*** il cui uso previsto o ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete ***esterni***.

Emendamento 41

Proposta di regolamento
Articolo 2 – paragrafo 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	5 bis. Il presente regolamento non si applica ai software liberi e open source,

compresi il codice sorgente e le versioni modificate, salvo laddove un software sia fornito nell'ambito di un'attività commerciale:

i) applicando un prezzo per un prodotto;

ii) mettendo a disposizione una piattaforma software che dipende da altri servizi che il fabbricante monetizza;

iii) utilizzando i dati personali generati dal software per motivi diversi dal solo miglioramento della sicurezza, della compatibilità o dell'interoperabilità del software;

iv) applicando un prezzo per i servizi di assistenza tecnica.

La conformità dei componenti liberi e open source dei prodotti è garantita dal fabbricante del prodotto in cui sono contenuti.

Emendamento 42

Proposta di regolamento
Articolo 2 – paragrafo 5 ter (nuovo)

Testo della Commissione	*Emendamento*
	5 ter. Il presente regolamento non si applica alle reti interne di un prodotto con elementi digitali laddove tali reti siano dotate di endpoint dedicati e siano completamente isolate e protette da una connessione dati esterna.

Emendamento 43

Proposta di regolamento
Articolo 2 – paragrafo 5 quater (nuovo)

Testo della Commissione	*Emendamento*
	5 quater. Il presente regolamento non si applica alle parti di ricambio destinate esclusivamente a sostituire parti difettose di prodotti con elementi digitali,

al fine di ripristinarne la funzionalità.

Emendamento 44

Proposta di regolamento
Articolo 3 – punto 1

Testo della Commissione	*Emendamento*
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;	1) "prodotto con elementi digitali": qualsiasi prodotto software o hardware, compresi i componenti software o hardware da immettere sul mercato separatamente;

Emendamento 45

Proposta di regolamento
Articolo 3 – punto 2

Testo della Commissione	*Emendamento*
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;	***soppresso***

Emendamento 46

Proposta di regolamento
Articolo 3 – punto 6 bis (nuovo)

Testo della Commissione	*Emendamento*
	6 bis) "software open source": software distribuito con una licenza che consente agli utenti di eseguirlo, copiarlo, distribuirlo, studiarlo, modificarlo e migliorarlo liberamente, nonché di integrarlo come componente in altri prodotti, fornirlo come servizio o fornire

	assistenza commerciale per lo stesso;

Emendamento 47

Proposta di regolamento
Articolo 3 – punto 18

Testo della Commissione	*Emendamento*
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;	*(Non concerne la versione italiana)*

Emendamento 48

Proposta di regolamento
Articolo 3 – punto 19

Testo della Commissione	*Emendamento*
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;	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 ***con riferimento agli obblighi del fabbricante***;

Emendamento 49

Proposta di regolamento
Articolo 3 – punto 23 bis (nuovo)

Testo della Commissione	*Emendamento*
	23 bis) "richiamo": un richiamo ai sensi dell'articolo 3, punto 22, del regolamento (UE) 2019/1020;

Emendamento 50

Proposta di regolamento
Articolo 3 – punto 26

Testo della Commissione	*Emendamento*
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;	***soppresso***

Emendamento 51

Proposta di regolamento
Articolo 3 – punto 31

Testo della Commissione	*Emendamento*
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;	31) "modifica sostanziale": una modifica del prodotto con elementi digitali***, esclusi gli aggiornamenti di sicurezza e manutenzione,*** 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;

Emendamento 52

Proposta di regolamento
Articolo 3 – punto 39

Testo della Commissione	*Emendamento*
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;	39) "vulnerabilità attivamente sfruttata": una vulnerabilità ***risolta con patch*** 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;

Emendamento 53

Proposta di regolamento
Articolo 3 – punto 40 bis (nuovo)

Testo della Commissione	*Emendamento*
	40 bis) "prodotto parzialmente completato con elementi digitali": un oggetto materiale che non è in grado di funzionare autonomamente e che è prodotto al solo scopo di essere incorporato o assemblato con un prodotto con elementi digitali o con un altro prodotto parzialmente completato con elementi digitali, e la cui conformità può essere efficacemente valutata solo tenendo conto del modo in cui è incorporato nel prodotto finale previsto con elementi digitali;

Emendamento 54

Proposta di regolamento
Articolo 3 – punto 40 ter (nuovo)

Testo della Commissione	*Emendamento*
	40 ter) "ciclo di vita": il periodo che va dal momento in cui un prodotto contemplato dal presente regolamento è immesso sul mercato o messo in servizio fino al momento in cui è scartato, compreso il tempo effettivo in cui esso può essere utilizzato e le fasi di trasporto, montaggio, smontaggio, smantellamento (messa fuori servizio), rottamazione o altre modifiche fisiche o digitali previste dal fabbricante.

Emendamento 55

Proposta di regolamento
Articolo 4 – paragrafo 1

Testo della Commissione	*Emendamento*
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.	1. Gli Stati membri non impediscono, per gli aspetti disciplinati dal presente regolamento, la messa a disposizione sul mercato di prodotti con elementi digitali ***o prodotti parzialmente completati con elementi digitali*** che sono conformi al presente regolamento.

Emendamento 56

Proposta di regolamento
Articolo 4 – paragrafo 2

Testo della Commissione	*Emendamento*
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.	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***, di un prototipo di un prodotto con elementi digitali o di un prodotto parzialmente completato con elementi digitali*** non conforme al presente regolamento ***a condizione che il prodotto con elementi digitali sia utilizzato esclusivamente per finalità di presentazione durante l'evento e che un'indicazione visibile specifichi chiaramente la non conformità al presente regolamento***.

Emendamento 57

Proposta di regolamento
Articolo 4 – paragrafo 3

Testo della Commissione	*Emendamento*
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	3. Gli Stati membri non impediscono la messa a disposizione di un ***prodotto con elementi digitali*** non finito ***o di un prototipo di un prodotto con elementi digitali*** non conforme al presente regolamento, a condizione che ***esso*** sia reso

un'indicazione visibile specifichi chiaramente che non è conforme al presente regolamento e non sarà disponibile sul mercato per fini diversi dalla prova.	disponibile solo ***in una versione non destinata all'uso in produzione*** 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.

Emendamento 58

Proposta di regolamento
Articolo 4 – paragrafo 3 bis (nuovo)

Testo della Commissione	*Emendamento*
	3 bis. Il presente regolamento non impedisce agli Stati membri di sottoporre i prodotti con elementi digitali a misure aggiuntive laddove tali prodotti specifici saranno utilizzati per scopi militari, di difesa o di sicurezza nazionale, conformemente al diritto nazionale e dell'Unione, e tali misure siano necessarie e proporzionate per il conseguimento di tali scopi.

Emendamento 59

Proposta di regolamento
Articolo 5 – punto 1

Testo della Commissione	*Emendamento*
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	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, ***ricevano i necessari aggiornamenti di sicurezza***, e

Emendamento 60

Proposta di regolamento
Articolo 6 – paragrafo 1

Testo della Commissione	*Emendamento*
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.	1. I prodotti con elementi digitali che appartengono a una categoria di cui all'allegato III sono considerati prodotti con elementi digitali critici. ***Solo*** 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. ***L'integrazione di un componente di classe di criticità superiore in un prodotto di criticità inferiore non modifica necessariamente il livello di criticità del prodotto in cui il componente è integrato.***

Emendamento 61

Proposta di regolamento
Articolo 6 – paragrafo 2 – lettera b

Testo della Commissione	*Emendamento*
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)];	b) l'uso previsto ***in applicazioni critiche*** in ambienti sensibili o da parte di soggetti essenziali del tipo di cui all'allegato [allegato I] della direttiva [direttiva XXX/XXXX (NIS2)];

Emendamento 62

Proposta di regolamento
Articolo 6 – paragrafo 2 – lettera c

Testo della Commissione	*Emendamento*
c) l'uso previsto per lo svolgimento di funzioni critiche o sensibili, come il trattamento dei dati personali;	c) l'uso previsto per lo svolgimento di funzioni critiche o sensibili, come il trattamento dei dati personali***, e la relativa***

portata;

Emendamento 63

Proposta di regolamento
Articolo 6 – paragrafo 4

Testo della Commissione	*Emendamento*
4. I prodotti con elementi digitali critici sono soggetti alle procedure di valutazione della conformità di cui all'articolo 24, paragrafi 2 e 3.	4. I prodotti con elementi digitali critici sono soggetti alle procedure di valutazione della conformità di cui all'articolo 24, paragrafi 2 e 3. ***In via eccezionale, le piccole e micro imprese possono ricorrere alla procedura di cui all'articolo 24, paragrafo 2.***

Emendamento 64

Proposta di regolamento
Articolo 6 – paragrafo 5 – parte introduttiva

Testo della Commissione	*Emendamento*
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:	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 ***possono*** 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:

Emendamento 65

Proposta di regolamento
Articolo 8 – paragrafo 1

Testo della Commissione	*Emendamento*
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.	1. I prodotti con elementi digitali ***o i prodotti parzialmente completati 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.

Emendamento 66

Proposta di regolamento
Articolo 8 – paragrafo 2

Testo della Commissione	*Emendamento*
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	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 [***dalle disposizioni applicabili***] 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]***.	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.

Emendamento 67

Proposta di regolamento
Articolo 8 – paragrafo 3

Testo della Commissione	*Emendamento*
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.	***soppresso***

Emendamento 68

Proposta di regolamento
Articolo 9

Testo della Commissione	*Emendamento*
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.	I prodotti macchina che rientrano nell'ambito di applicazione del regolamento [proposta di regolamento sui prodotti macchina], che sono ***prodotti con elementi digitali o*** prodotti con elementi digitali ***parzialmente completati*** 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.

Emendamento 69

Proposta di regolamento
Articolo 10 – paragrafo -1 (nuovo)

Testo della Commissione	*Emendamento*
	-1. I fabbricanti di software considerati come microimprese ai sensi della raccomandazione 2003/361/CE della Commissione fanno il possibile per conformarsi ai requisiti di cui al presente regolamento nei sei mesi successivi all'immissione sul mercato del software. La presente disposizione non si applica ai prodotti con elementi digitali altamente critici.

Emendamento 70

Proposta di regolamento
Articolo 10 – paragrafo 1

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

Emendamento 71

Proposta di regolamento
Articolo 10 – paragrafo 4

Testo della Commissione	*Emendamento*
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.	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. ***Spetta ai fabbricanti garantire*** che tali componenti non compromettano la sicurezza del prodotto con elementi digitali.

Emendamento 72

Proposta di regolamento
Articolo 10 – paragrafo 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	4 bis. I fabbricanti di componenti forniscono le informazioni e la documentazione necessarie per conformarsi ai requisiti di cui al presente regolamento quando forniscono tali componenti al fabbricante di prodotti finiti. Tali informazioni sono fornite gratuitamente.

Emendamento 73

Proposta di regolamento
Articolo 10 – paragrafo 6 – comma 1

Testo della Commissione	*Emendamento*
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.	All'atto dell'immissione sul mercato di un prodotto con elementi digitali e per la durata prevista del prodotto ***al momento della sua immissione sul mercato*** o per un periodo di cinque anni dall'immissione sul mercato del prodotto, a seconda di quale sia il periodo più ***lungo***, 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***, per quanto in loro potere***.

Emendamento 74

Proposta di regolamento
Articolo 10 – paragrafo 7 – comma 3 bis (nuovo)

Testo della Commissione	*Emendamento*
	Se il software è aggiornato, il fabbricante non è tenuto a effettuare un'altra valutazione di conformità del prodotto con elementi digitali, a meno che l'aggiornamento del software non comporti una modifica sostanziale del prodotto con elementi digitali ai sensi dell'articolo 3, punto 31, del presente regolamento.

Emendamento 75

Proposta di regolamento
Articolo 10 – paragrafo 9

Testo della Commissione	*Emendamento*
9. I fabbricanti si assicurano che siano predisposte le procedure necessarie affinché i prodotti con elementi digitali fabbricati nell'ambito di una produzione in	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.	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. ***Qualora si rendano disponibili nuove conoscenze, tecniche o norme che non erano disponibili al momento della progettazione di un prodotto di serie, il fabbricante può valutare la possibilità di apportare periodicamente tali miglioramenti alle generazioni future del prodotto.***

Emendamento 76

Proposta di regolamento
Articolo 10 – paragrafo 9 bis (nuovo)

Testo della Commissione	*Emendamento*
	9 bis. I fabbricanti comunicano pubblicamente la durata prevista dei loro prodotti in modo chiaro e comprensibile.

Emendamento 77

Proposta di regolamento
Articolo 10 – paragrafo 12

Testo della Commissione	*Emendamento*
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	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 ***lungo***, 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.	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.

Emendamento 78

Proposta di regolamento
Articolo 11 – paragrafo 1

Testo della Commissione	*Emendamento*
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.***	1. Il fabbricante notifica all'ENISA, senza indebito ritardo e comunque entro ***48*** ore dal momento in cui ne è venuto a conoscenza, ***mediante una segnalazione preventiva,*** qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali.

Emendamento 79

Proposta di regolamento
Articolo 11 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. Il fabbricante fornisce all'ENISA, senza indebito ritardo dal momento in cui è venuto a conoscenza del fatto che la

vulnerabilità attivamente sfruttata ha un impatto significativo sulla sicurezza del prodotto con elementi digitali, maggiori informazioni su tale vulnerabilità sfruttata.

Emendamento 80

Proposta di regolamento
Articolo 11 – paragrafo 1 ter (nuovo)

Testo della Commissione	*Emendamento*
	1 ter. Tutte le altre vulnerabilità che non hanno un impatto significativo sulla sicurezza del prodotto con elementi digitali sono notificate all'ENISA una volta affrontate.

Emendamento 81

Proposta di regolamento
Articolo 11 – paragrafo 1 quater (nuovo)

Testo della Commissione	*Emendamento*
	1 quater. La notifica include i dettagli relativi a tale vulnerabilità e, se del caso, le misure correttive o di attenuazione adottate, nonché le misure di attenuazione dei rischi raccomandate. 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 immediatamente l'autorità di vigilanza del mercato in merito all'esistenza di una vulnerabilità e, se del caso, alle misure di attenuazione dei rischi potenziali. Qualora a una vulnerabilità notificata non corrispondano misure correttive o di

	attenuazione, l'ENISA garantisce che le informazioni sulla vulnerabilità notificata siano condivise nel rispetto di rigorosi protocolli di sicurezza e limitatamente a quanto necessario.

Emendamento 82

Proposta di regolamento
Articolo 11 – paragrafo 2

Testo della Commissione	*Emendamento*
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.	2. Il fabbricante notifica all'ENISA, senza indebito ritardo e comunque entro 24 ore dal momento in cui ne è venuto a conoscenza, ***mediante una segnalazione preventiva,*** qualsiasi incidente che abbia un impatto ***significativo*** sulla sicurezza del prodotto con elementi digitali. ***Il fabbricante comunica inoltre all'ENISA, senza indebito ritardo e comunque entro 72 ore dal momento in cui è venuto a conoscenza dell'incidente significativo relativo al prodotto con elementi digitali, maggiori informazioni sul tale incidente significativo.*** 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 ***immediatamente*** l'autorità di vigilanza del mercato degli incidenti ***significativi*** notificati. La notifica dell'incidente comprende ***le informazioni strettamente necessarie per informare l'autorità competente dell'incidente e, ove pertinente e proporzionato al rischio,*** 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. ***La sola notifica non espone il soggetto che la effettua a una maggiore responsabilità.***

Emendamento 83

Proposta di regolamento
Articolo 11 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. Gli operatori economici considerati anche come soggetti essenziali o importanti ai sensi della direttiva NIS2 e che trasmettono la notifica dell'incidente a norma di tale direttiva dovrebbero presumersi conformi ai requisiti di cui al paragrafo 2 del presente articolo.

Emendamento 84

Proposta di regolamento
Articolo 11 – paragrafo 3

Testo della Commissione	*Emendamento*
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.	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 ***significativi*** e delle crisi di cibersicurezza su vasta scala a livello operativo.

Emendamento 85

Proposta di regolamento
Articolo 11 – paragrafo 4

Testo della Commissione	*Emendamento*
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	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.	all'incidente ***significativo, ove opportuno e qualora sia probabile che essi ne subiscano gli effetti negativi,*** e, se necessario, ***in merito alle misure di attenuazione dei rischi e*** alle misure correttive che essi possono adottare per attenuarne l'impatto ***per quanto concerne i dati eventualmente interessati e i danni potenziali***.

Emendamento 86

Proposta di regolamento
Articolo 11 – paragrafo 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	4 bis. Gli obblighi di cui ai paragrafi 1, 2 e 4 si applicano per l'intera durata del prodotto. Per tutta la durata prevista del prodotto, il fabbricante fornisce gratuitamente aggiornamenti di sicurezza che si applicano solo ai prodotti con elementi digitali per i quali il fabbricante ha redatto una dichiarazione di conformità UE, a norma dell'articolo 20 del presente regolamento.

Emendamento 87

Proposta di regolamento
Articolo 11 – paragrafo 5

Testo della Commissione	*Emendamento*
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.	5. La Commissione***, previa consultazione dei portatori di interessi e dei CSIRT,*** 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 ***tengono conto delle norme europee e internazionali e*** sono adottati secondo la procedura d'esame di cui all'articolo 51, paragrafo 2.

Emendamento 88

Proposta di regolamento
Articolo 11 – paragrafo 6

Testo della Commissione	*Emendamento*
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.	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 ***14*** della direttiva ***(UE) 2022/2555***. La prima relazione di questo tipo è presentata entro 24 mesi dall'inizio dell'applicazione degli obblighi di cui ai paragrafi 1 e 2.

Emendamento 89

Proposta di regolamento
Articolo 11 – paragrafo 7

Testo della Commissione	*Emendamento*
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.	7. Quando è individuata una vulnerabilità in un componente, compreso un componente open source, integrato nel prodotto con elementi digitali, i fabbricanti la segnalano***, unitamente alla misura correttiva o di attenuazione adottata,*** alla persona o al soggetto che si occupa della manutenzione di tale componente. ***Ciò non esonera il fabbricante dall'obbligo di mantenere la conformità del prodotto ai requisiti del presente regolamento né crea obblighi per gli sviluppatori di componenti liberi e open source che non hanno alcun rapporto contrattuale con il suddetto fabbricante.***

Emendamento 90

Proposta di regolamento
Articolo 12 – paragrafo 3 – parte introduttiva

Testo della Commissione	*Emendamento*
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:	3. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fabbricante. ***Su richiesta, fornisce una copia del mandato alle autorità di vigilanza del mercato.*** Tale mandato consente al rappresentante autorizzato di svolgere almeno i seguenti compiti:

Emendamento 91

Proposta di regolamento
Articolo 12 – paragrafo 3 – lettera a bis (nuova)

Testo della Commissione	*Emendamento*
	a bis) qualora il rappresentante autorizzato abbia motivo di credere che il prodotto con elementi digitali in questione presenta un rischio di cibersicurezza, ne informa il fabbricante;

Emendamento 92

Proposta di regolamento
Articolo 12 – paragrafo 3 – lettera b

Testo della Commissione	*Emendamento*
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;	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 sicurezza e*** la conformità del prodotto con elementi digitali ***in una lingua che possa essere facilmente compresa da tale autorità***;

Emendamento 93

Proposta di regolamento
Articolo 12 – paragrafo 3 – lettera c

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

Emendamento 94

Proposta di regolamento
Articolo 13 – paragrafo 2 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	c bis) tutti i documenti che dimostrano la conformità ai requisiti di cui al presente articolo siano stati ricevuti dal fabbricante e siano a disposizione a fini di ispezione per un periodo di dieci anni.

Emendamento 95

Proposta di regolamento
Articolo 13 – paragrafo 3

Testo della Commissione	*Emendamento*
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.	3. Qualora ritenga o abbia motivo di credere***, sulla base delle informazioni in suo possesso,*** 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.

Emendamento 96

Proposta di regolamento
Articolo 13 – paragrafo 4

Testo della Commissione	*Emendamento*
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.	*(Non concerne la versione italiana)*

Emendamento 97

Proposta di regolamento
Articolo 13 – paragrafo 6 – comma 1

Testo della Commissione	*Emendamento*
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.	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. ***Sulla base di una valutazione dei rischi, i distributori e gli utilizzatori finali sono informati tempestivamente della non conformità e delle misure di attenuazione dei rischi che essi possono adottare.***

Emendamento 98

Proposta di regolamento
Articolo 14 – paragrafo 2 – lettera b bis (nuova)

Testo della Commissione	*Emendamento*
	b bis) abbiano ricevuto dal fabbricante o dall'importatore tutte le informazioni e la documentazione richieste dal presente regolamento.

Emendamento 99

Proposta di regolamento
Articolo 16 – comma 1

Testo della Commissione	*Emendamento*
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.	Una persona fisica o giuridica, diversa dal fabbricante, dall'importatore o dal distributore, che***, nello svolgimento di un'attività professionale,*** apporta una modifica sostanziale al prodotto con elementi digitali ***e lo mette a disposizione sul mercato*** è considerata un fabbricante ai fini del presente regolamento.

Emendamento 100

Proposta di regolamento
Articolo 18 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. Conformemente all'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, la Commissione richiede a una o più organizzazioni europee di normazione di redigere norme armonizzate relative ai requisiti di cui all'allegato I.

Emendamento 101

Proposta di regolamento
Articolo 18 – paragrafo 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	4 bis. Conformemente all'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, nell'elaborare la richiesta di normazione dei prodotti rientranti nell'ambito di applicazione del presente regolamento, la Commissione mira alla massima armonizzazione con le norme internazionali in materia di cibersicurezza vigenti o la cui pubblicazione è imminente. Nei primi tre anni successivi alla data di applicazione del presente regolamento, alla Commissione è conferito il potere di dichiarare una norma internazionale esistente come conforme ai requisiti del presente regolamento, senza alcuna modifica europea, a condizione che il rispetto di tale norma rafforzi in misura sufficiente la sicurezza dei prodotti con elementi digitali e che la norma sia pubblicata in una versione separata da una delle organizzazioni europee di normazione.

Emendamento 102

Proposta di regolamento
Articolo 19

Testo della Commissione	*Emendamento*
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***	***1. Alla*** Commissione ***è conferito il potere di adottare atti di esecuzione che stabiliscono specifiche comuni relative ai*** requisiti ***tecnici che forniscono i mezzi per*** soddisfare ***i requisiti essenziali in materia di sicurezza e tutela della salute di cui all'allegato I per i prodotti rientranti nell'ambito di applicazione del presente regolamento. Tali atti di esecuzione sono adottati solo laddove siano soddisfatte le condizioni seguenti:***

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***.

a) la Commissione ***ha richiesto, a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, a una o più*** organizzazioni europee di normazione ***di redigere una norma armonizzata per*** i requisiti essenziali di cui all'allegato I ***e:***

i) la richiesta non è stata accolta; o

ii) le norme armonizzate corrispondenti a tale richiesta non sono fornite entro il termine stabilito conformemente all'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012; o

iii) le norme armonizzate non sono conformi alla richiesta; e

b) nessun riferimento a norme armonizzate che contemplano i requisiti di cui all'allegato I è stato pubblicato nella Gazzetta ufficiale dell'Unione europea conformemente al regolamento (UE) n. 1025/2012 e non si prevede la pubblicazione di tale riferimento entro un termine ragionevole.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo ***48***, paragrafo ***3***.

Emendamento 103

Proposta di regolamento
Articolo 19 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. Prima di preparare il progetto di atto di esecuzione di cui al paragrafo 3, la Commissione informa il comitato di cui all'articolo 22 del regolamento (UE) n. 1025/2012 di ritenere soddisfatte le condizioni di cui al paragrafo 3.

Emendamento 104

Proposta di regolamento
Articolo 19 – paragrafo 1 ter (nuovo)

Testo della Commissione	*Emendamento*
	1 ter. Nel preparare il progetto di atto di esecuzione di cui al paragrafo 1, la Commissione tiene conto dei pareri degli organi competenti o del gruppo di esperti e consulta debitamente tutti i portatori di interessi.

Emendamento 105

Proposta di regolamento
Articolo 19 – paragrafo 1 quater (nuovo)

Testo della Commissione	*Emendamento*
	1 quater. Qualora una norma armonizzata sia adottata da un'organizzazione europea di normazione e proposta alla Commissione al fine di pubblicarne il riferimento nella Gazzetta ufficiale dell'Unione europea, la Commissione valuta la norma armonizzata conformemente al regolamento (UE) n. 1025/2012. Quando il riferimento a una norma armonizzata è pubblicato nella Gazzetta ufficiale dell'Unione europea, la Commissione abroga gli atti di esecuzione di cui al paragrafo 1, o parti di essi, che riguardano gli stessi requisiti contemplati da tale norma armonizzata.

Emendamento 106

Proposta di regolamento
Articolo 19 – paragrafo 1 quinquies (nuovo)

Testo della Commissione	*Emendamento*
	1 quinquies. Se uno Stato membro ritiene che una specifica comune non soddisfi interamente i requisiti di cui all'allegato I, ne informa la Commissione presentando una spiegazione dettagliata. La Commissione valuta tale spiegazione dettagliata e può, se del caso, modificare l'atto di esecuzione che stabilisce la specifica comune in questione.

Emendamento 107

Proposta di regolamento
Articolo 20 – paragrafo 2

Testo della Commissione	*Emendamento*
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.	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 ***opportunamente*** aggiornata. È resa disponibile ***in una*** lingua ***che possa essere facilmente compresa dalle autorità dello*** Stato membro sul cui mercato il prodotto con elementi digitali è immesso o messo a disposizione.

Emendamento 108

Proposta di regolamento
Articolo 20 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 20 bis
	Dichiarazione di incorporazione UE per prodotti con elementi digitali parzialmente completati
	1. La dichiarazione di incorporazione UE è redatta dai fabbricanti in conformità

	dell'articolo 10, paragrafo 7, e attesta il rispetto dei requisiti essenziali pertinenti di cui all'allegato I.
	2. La dichiarazione di incorporazione UE ha la struttura tipo di cui all'allegato IV bis (nuovo). Tale dichiarazione è opportunamente aggiornata. È resa disponibile nella lingua o nelle lingue richieste dallo Stato membro sul cui mercato il prodotto con elementi digitali parzialmente completato è immesso o messo a disposizione.
	3. Se al prodotto con elementi digitali parzialmente completato si applicano più atti dell'Unione che prescrivono una dichiarazione di incorporazione UE, è redatta un'unica dichiarazione di incorporazione 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. 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 incorporazione UE di cui all'allegato IV bis (nuovo) per tenere conto degli sviluppi tecnologici.

Emendamento 109

Proposta di regolamento
Articolo 22 – paragrafo 1

Testo della Commissione	*Emendamento*
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	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.	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. ***In quest'ultimo caso, la sezione pertinente del sito web è facilmente e direttamente accessibile ai consumatori.***

Emendamento 110

Proposta di regolamento
Articolo 22 – paragrafo 3

Testo della Commissione	*Emendamento*
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.	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 ***ai consumatori*** un rischio o un impiego particolare stabilito negli atti di esecuzione di cui al paragrafo 6.

Emendamento 111

Proposta di regolamento
Articolo 22 – paragrafo 5

Testo della Commissione	*Emendamento*
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.	5. Gli Stati membri si avvalgono dei meccanismi esistenti per garantire un'applicazione corretta ***e armonizzata*** del regime che disciplina la marcatura CE e promuovono le azioni opportune ***e coordinate*** 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.

Emendamento 112

Proposta di regolamento
Articolo 22 – paragrafo 6

Testo della Commissione	*Emendamento*
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***.	6. La Commissione può, mediante atti ***delegati***, stabilire specifiche tecniche per ***i sistemi di etichettatura, comprese le etichette armonizzate,*** i pittogrammi o qualsiasi altro marchio relativo alla sicurezza dei prodotti con elementi digitali e meccanismi per promuoverne l'uso ***tra le imprese e i consumatori, nonché per sensibilizzare il pubblico in merito alla sicurezza dei prodotti con elementi digitali***. Tali atti ***delegati*** sono adottati secondo la procedura di cui all'articolo ***50***.

Emendamento 113

Proposta di regolamento
Articolo 22 – paragrafo 6 bis (nuovo)

Testo della Commissione	*Emendamento*
	6 bis. Un prodotto con elementi digitali parzialmente completato non reca la marcatura CE prevista dal presente regolamento, fatte salve le disposizioni in materia di marcatura derivanti da altre normative dell'Unione applicabili.

Emendamento 114

Proposta di regolamento
Articolo 22 – paragrafo 6 ter (nuovo)

Testo della Commissione	*Emendamento*
	6 ter. La Commissione adotta orientamenti e fornisce consulenza agli operatori economici, in particolare a quelli che si qualificano come PMI, comprese le microimprese, sull'attuazione del presente regolamento. In particolare, gli orientamenti e la consulenza mirano a

	semplificare e limitare gli oneri amministrativi e finanziari, garantendo al contempo un'applicazione efficace e coerente del presente regolamento, conformemente all'obiettivo generale di garantire la sicurezza dei prodotti e la protezione dei consumatori. La Commissione dovrebbe consultare i portatori di interessi pertinenti con competenze nell'ambito della cibersicurezza.

Emendamento 115

Proposta di regolamento
Articolo 23 – paragrafo 2

Testo della Commissione	*Emendamento*
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***.	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 ***lungo***.

Emendamento 116

Proposta di regolamento
Articolo 23 – paragrafo 3

Testo della Commissione	*Emendamento*
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.	3. Per i prodotti con elementi digitali 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.

Emendamento 117

Proposta di regolamento
Articolo 23 – paragrafo 5

Testo della Commissione	*Emendamento*
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.	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. ***La Commissione si adopera per ridurre al minimo gli oneri amministrativi, segnatamente per le microimprese e le piccole e medie imprese.***

Emendamento 118

Proposta di regolamento
Articolo 24 – paragrafo 1 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	c bis) un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 18, paragrafo 4, del regolamento (UE) 2019/881.

Emendamento 119

Proposta di regolamento
Articolo 24 – paragrafo 3 – lettera b

Testo della Commissione	*Emendamento*
b) la valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'allegato VI**.**	b) la valutazione della conformità basata sulla garanzia della qualità totale (basata sul modulo H) di cui all'allegato VI***; o***

Emendamento 120

Proposta di regolamento
Articolo 24 – paragrafo 3 – lettera b bis (nuova)

Testo della Commissione	*Emendamento*
	b bis) se del caso, un sistema europeo di certificazione della cibersicurezza con un livello di affidabilità "sostanziale" o "elevato" ai sensi del regolamento (UE) 2019/881.

Emendamento 121

Proposta di regolamento
Articolo 24 – paragrafo 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	4 bis. Per i prodotti cui si applica la normativa di armonizzazione dell'Unione in base al nuovo quadro normativo, il fabbricante segue la pertinente valutazione della conformità prevista da tali atti giuridici. A tali prodotti si applicano i requisiti di cui al capo III.

Emendamento 122

Proposta di regolamento
Articolo 24 – paragrafo 5

Testo della Commissione	*Emendamento*
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.	5. Gli organismi notificati tengono conto degli interessi e delle esigenze specifici ***delle microimprese e*** delle piccole e medie imprese 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. ***La Commissione adotta misure intese a garantire procedure più accessibili e a prezzi più abbordabili nonché un adeguato sostegno finanziario nel quadro dei programmi esistenti dell'Unione, in particolare al fine di alleggerire gli oneri***

a carico delle microimprese e delle piccole e medie imprese.

Emendamento 123

Proposta di regolamento
Articolo 24 – paragrafo 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	5 bis. Per i prodotti con elementi digitali rientranti nell'ambito di applicazione del presente regolamento e immessi sul mercato o messi in servizio da enti creditizi disciplinati dalla direttiva 2013/36/UE, la valutazione della conformità è effettuata nell'ambito della procedura di cui agli articoli da 97 a 101 di tale direttiva.

Emendamento 124

Proposta di regolamento
Articolo 24 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 24 bis
	Quando i prodotti con elementi digitali sono dotati di hardware o software equivalenti, un modello di prodotto può essere rappresentativo di una famiglia di prodotti ai fini delle seguenti procedure di valutazione della conformità:
	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.

Emendamento 125

Proposta di regolamento
Articolo 27 – paragrafo 5

Testo della Commissione	*Emendamento*
5. L'autorità di notifica salvaguarda la riservatezza delle informazioni ottenute.	5. L'autorità di notifica salvaguarda la riservatezza delle informazioni ottenute***, compresi i diritti di proprietà intellettuale, le informazioni commerciali riservate e i segreti commerciali***.

Emendamento 126

Proposta di regolamento
Articolo 27 – paragrafo 6 bis (nuovo)

Testo della Commissione	*Emendamento*
	6 bis. L'autorità di notifica riduce al minimo gli oneri burocratici e le tariffe, in particolare per le PMI.

Emendamento 127

Proposta di regolamento
Articolo 29 – paragrafo 7 bis (nuovo)

Testo della Commissione	*Emendamento*
	7 bis. Gli Stati membri e la Commissione adottano misure adeguate onde garantire una disponibilità sufficiente di professionisti qualificati, al fine di ridurre al minimo gli ostacoli nelle attività degli organismi di valutazione della conformità.

Emendamento 128

Proposta di regolamento
Articolo 29 – paragrafo 10

Testo della Commissione	*Emendamento*
10. Il personale dell'organismo di	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.	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 ***intellettuale, le informazioni commerciali riservate e i segreti commerciali***. L'organismo di valutazione della conformità dispone di procedure documentate che garantiscono la conformità al presente paragrafo.

Emendamento 129

Proposta di regolamento
Articolo 29 – paragrafo 12

Testo della Commissione	*Emendamento*
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.	12. Gli organismi di valutazione della conformità operano secondo modalità e condizioni coerenti, eque e ragionevoli ***in conformità dell'articolo 37, paragrafo 2***, tenendo conto in particolare degli interessi delle ***microimprese e delle piccole e media imprese*** in relazione alle tariffe.

Emendamento 130

Proposta di regolamento
Articolo 36 – paragrafo 3

Testo della Commissione	*Emendamento*
3. La Commissione garantisce la riservatezza di tutte le informazioni ***sensibili*** raccolte nel corso delle sue indagini.	3. La Commissione garantisce la riservatezza di tutte le informazioni***, compresi i diritti di proprietà intellettuale, le informazioni commerciali riservate e i segreti commerciali,*** raccolte nel corso delle sue indagini.

Emendamento 131

Proposta di regolamento
Articolo 37 – paragrafo 2

Testo della Commissione	*Emendamento*
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.	2. Le valutazioni della conformità sono eseguite in modo proporzionato, evitando oneri inutili per gli operatori economici***, in particolare per le PMI***. 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 ***e dell'esposizione al rischio del tipo e*** della tecnologia del prodotto in questione e della natura di massa o seriale del processo produttivo.

Emendamento 132

Proposta di regolamento
Articolo 37 – paragrafo 5

Testo della Commissione	*Emendamento*
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.	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 ***limita,*** sospende o ritira il certificato.

Emendamento 133

Proposta di regolamento
Articolo 40 – paragrafo 1

Testo della Commissione	*Emendamento*
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	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.	organismi notificati***, tenendo altresì conto della necessità di ridurre gli oneri burocratici e le tariffe***.

Emendamento 134

Proposta di regolamento
Articolo 40 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Gli Stati membri garantiscono che gli organismi da essi notificati partecipino al lavoro di tale gruppo, direttamente o mediante rappresentanti designati.	2. Gli Stati membri garantiscono che gli organismi da essi notificati partecipino al lavoro di tale gruppo, direttamente o mediante rappresentanti designati***, tenendo altresì conto della necessità di ridurre gli oneri burocratici e le tariffe***.

Emendamento 135

Proposta di regolamento
Articolo 41 – paragrafo 3

Testo della Commissione	*Emendamento*
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.	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 ***efficacemente*** con l'ENISA. ***Le autorità di vigilanza del mercato possono chiedere all'ENISA di fornire consulenza tecnica su questioni relative all'attuazione e all'applicazione del presente regolamento, anche nel corso delle indagini di cui all'articolo 43, quando le autorità di vigilanza del mercato possono chiedere all'ENISA di fornire valutazioni non vincolanti sulla conformità dei prodotti con elementi***

digitali.

Emendamento 136

Proposta di regolamento
Articolo 41 – paragrafo 7

Testo della Commissione	*Emendamento*
7. La Commissione agevola lo scambio di esperienze tra le autorità di vigilanza del mercato designate.	7. La Commissione agevola lo scambio ***regolare e strutturato*** di esperienze tra le autorità di vigilanza del mercato designate***, anche attraverso un apposito gruppo di cooperazione amministrativa (ADCO) istituito a norma del paragrafo 11 del presente articolo***.

Emendamento 137

Proposta di regolamento
Articolo 41 – paragrafo 8

Testo della Commissione	*Emendamento*
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***.	8. ***La Commissione adotta orientamenti e fornisce*** agli operatori economici ***consulenza, in particolare a quelli che si qualificano come PMI, comprese le microimprese,*** sull'attuazione del presente regolamento***. In particolare***, ***gli orientamenti e la consulenza mirano a semplificare e limitare l'onere amministrativo e finanziario, garantendo al contempo un'applicazione efficace e coerente, conformemente all'obiettivo generale di garantire la sicurezza dei prodotti e la protezione dei consumatori***.

Emendamento 138

Proposta di regolamento
Articolo 41 – paragrafo 8 bis (nuovo)

Testo della Commissione	*Emendamento*
	8 bis. Le autorità di vigilanza del mercato devono essere preparate a ricevere dai consumatori i reclami a norma dell'articolo 11 del regolamento 2019/1020, anche istituendo meccanismi chiari e accessibili per agevolare la segnalazione di vulnerabilità, incidenti e minacce informatiche.

Emendamento 139

Proposta di regolamento
Articolo 41 – paragrafo 11

Testo della Commissione	*Emendamento*
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.	11. Per l'applicazione uniforme del presente regolamento***, l'agevolazione della cooperazione strutturata in relazione all'attuazione del presente regolamento e la semplificazione delle pratiche delle autorità di vigilanza del mercato all'interno dell'Unione,*** è istituito un apposito gruppo di cooperazione amministrativa (ADCO) a norma dell'articolo 30, paragrafo 2, del regolamento (UE) 2019/1020. Tale ADCO è ***responsabile, in particolare, dei compiti di cui all'articolo 32, paragrafo 2, del regolamento (UE) 2019/1020 ed è*** composto da rappresentanti delle autorità di vigilanza del mercato designate e ***dell'ENISA e***, se del caso, da rappresentanti degli uffici unici di collegamento. ***L'ADCO si riunisce periodicamente e, se necessario, su richiesta debitamente giustificata della Commissione, dell'ENISA o di uno Stato membro e coordina la propria azione con altre attività dell'Unione esistenti in materia di vigilanza del mercato e sicurezza dei consumatori e, se del caso, collabora e scambia informazioni con altre reti, gruppi e organismi dell'Unione. L'ADCO può invitare a partecipare alle***

	sue riunioni esperti e altri terzi, comprese le organizzazioni dei consumatori.

Emendamento 140

Proposta di regolamento
Articolo 41 – paragrafo 11 bis (nuovo)

Testo della Commissione	*Emendamento*
	11 bis. Per i prodotti con elementi digitali che rientrano nell'ambito di applicazione del presente regolamento, distribuiti, messi in servizio o utilizzati da enti finanziari disciplinati dalla legislazione dell'Unione sui servizi finanziari pertinente, ai fini del presente regolamento l'autorità di vigilanza del mercato è l'autorità pertinente responsabile della vigilanza finanziaria di tali enti ai sensi di tale legislazione.

Emendamento 141

Proposta di regolamento
Articolo 42 – comma unico

Testo della Commissione	*Emendamento*
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.	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. ***Se del caso, e conformemente all'articolo 52, paragrafo 1, lettera a), ciò avviene in un ambiente sicuro e controllato stabilito dal fabbricante.***

Emendamento 142

Proposta di regolamento
Articolo 43 – paragrafo 1 – comma 2

Testo della Commissione	*Emendamento*
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.	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 ***o rappresenta altrimenti una minaccia alla sicurezza nazionale***, essa chiede senza indugio all'operatore economico 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. ***Prima della suddetta valutazione, se necessario, tenuto conto della rilevanza del rischio di cibersicurezza, l'autorità di vigilanza del mercato può richiedere all'operatore interessato di sospendere o limitare immediatamente la disponibilità del prodotto sul mercato per il periodo della valutazione di cui sopra.***

Emendamento 143

Proposta di regolamento
Articolo 43 – paragrafo 4 – comma 1

Testo della Commissione	*Emendamento*
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.	Qualora il fabbricante di un prodotto con elementi digitali non adotti misure correttive adeguate entro il termine di cui al paragrafo 1, secondo comma, ***o le autorità pertinenti degli Stati membri ritengano che il prodotto rappresenti una minaccia alla sicurezza nazionale,*** 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.

Emendamento 144

Proposta di regolamento
Articolo 45 – paragrafo 1

Testo della Commissione	*Emendamento*
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.	1. Se la Commissione ha motivi sufficienti per ritenere, anche sulla base delle informazioni fornite ***dalle autorità competenti degli Stati membri, dai gruppi di intervento per la sicurezza informatica in caso di incidente (Computer Security Incident Response Teams – CSIRT) designati o istituiti ai sensi della direttiva (UE) 2022/2555 o*** dall'ENISA, che un prodotto con elementi digitali che presenta un rischio di cibersicurezza significativo non sia conforme ai requisiti stabiliti nel presente regolamento, ***chiede*** alle autorità di vigilanza del mercato competenti di effettuare una valutazione della conformità e di seguire le procedure di cui all'articolo 43.

Emendamento 145

Proposta di regolamento
Articolo 45 – paragrafo 2

Testo della Commissione	*Emendamento*
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	2. In circostanze che giustifichino un intervento immediato per preservare il buon funzionamento del mercato interno e qualora la Commissione abbia motivi 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 ***chiede*** all'ENISA di effettuare una valutazione della conformità. La Commissione ne informa le autorità di vigilanza del mercato competenti. Gli operatori economici

operatori economici interessati cooperano, per quanto necessario, con l'ENISA.

interessati cooperano, per quanto necessario, con l'ENISA.

Emendamento 146

Proposta di regolamento
Articolo 46 – paragrafo 1

Testo della Commissione	*Emendamento*
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.	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 ***(UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2),*** o per altri aspetti della tutela dell'interesse pubblico, essa chiede all'operatore ***economico*** 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.

Emendamento 147

Proposta di regolamento
Articolo 46 – paragrafo 2

Testo della Commissione	*Emendamento*
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.	2. Il fabbricante o altri operatori ***economici*** 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.

Emendamento 148

Proposta di regolamento
Articolo 46 – paragrafo 6

Testo della Commissione	*Emendamento*
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.	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 ***chiede*** 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.

Emendamento 149

Proposta di regolamento
Articolo 46 – paragrafo 7

Testo della Commissione	*Emendamento*
7. In circostanze ***eccezionali*** che giustifichino un intervento immediato per preservare il buon funzionamento del mercato interno e qualora la Commissione	7. In circostanze che giustifichino un intervento immediato per preservare il buon funzionamento del mercato interno e qualora la Commissione abbia motivi

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.

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 ***chiede*** 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.

Emendamento 150

Proposta di regolamento
Articolo 48 – paragrafo 1

Testo della Commissione	*Emendamento*
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.	1. Le autorità di vigilanza del mercato ***realizzano regolarmente attività congiunte*** con altre autorità competenti 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. ***Tali attività comprendono ispezioni sui prodotti acquistati sotto un'identità di copertura.***

Emendamento 151

Proposta di regolamento
Articolo 48 – paragrafo 2

Testo della Commissione	*Emendamento*
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	2. La Commissione o l'ENISA ***propongono*** 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.	nell'ambito di applicazione del presente regolamento ai requisiti stabiliti da quest'ultimo.

Emendamento 152

Proposta di regolamento
Articolo 49 – paragrafo 1

Testo della Commissione	*Emendamento*
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.	1. Le autorità di vigilanza del mercato ***conducono regolarmente*** azioni di controllo ***simultanee*** 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.

Emendamento 153

Proposta di regolamento
Articolo 49 – paragrafo 2

Testo della Commissione	*Emendamento*
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.	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 ***rende disponibili al pubblico***, ***se*** del ***caso,*** i risultati aggregati.

Emendamento 154

Proposta di regolamento
Articolo 49 – paragrafo 3

Testo della Commissione	*Emendamento*
3. L'ENISA ***può individuare***, nell'esecuzione dei suoi compiti, anche sulla base delle notifiche ricevute conformemente all'articolo 11, paragrafi 1	3. L'ENISA ***individua***, nell'esecuzione dei suoi compiti, anche sulla base delle notifiche ricevute conformemente all'articolo 11, paragrafi 1 e 2, categorie di

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.	prodotti per le quali ***sono*** 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.

Emendamento 155

Proposta di regolamento
Articolo 49 – paragrafo 5

Testo della Commissione	*Emendamento*
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.	5. Le autorità di vigilanza del mercato ***invitano*** i funzionari della Commissione e altre persone di accompagnamento autorizzate dalla Commissione a partecipare alle indagini a tappeto.

Emendamento 156

Proposta di regolamento
Articolo 49 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 49 bis
	Fornitura di assistenza tecnica
	1. La Commissione nomina, mediante un atto di esecuzione, un gruppo di esperti incaricato di fornire assistenza tecnica alle autorità di vigilanza del mercato su questioni relative all'attuazione e all'applicazione del presente regolamento. L'atto di esecuzione specifica, tra l'altro, i dettagli relativi alla composizione del gruppo, al suo funzionamento e alla remunerazione dei relativi membri. In particolare, il gruppo di esperti fornisce valutazioni non vincolanti di prodotti con elementi digitali su richiesta di un'autorità di vigilanza del mercato che sta conducendo un'indagine ai sensi dell'articolo 43 e dell'elenco dei

prodotti critici con elementi digitali di cui all'allegato II, nonché sull'eventuale necessità di aggiornare tale elenco.

2. Il gruppo di esperti è composto da esperti indipendenti nominati dalla Commissione per un mandato triennale rinnovabile sulla base delle loro competenze scientifiche o tecniche nel settore.

3. La Commissione nomina un numero di esperti ritenuto sufficiente a soddisfare le esigenze previste.

4. La Commissione adotta le misure necessarie per gestire e prevenire eventuali conflitti di interesse. Le dichiarazioni di interessi dei membri del gruppo di esperti sono rese pubbliche.

5. Gli esperti nominati svolgono i loro compiti con il massimo livello di professionalità, indipendenza, imparzialità e oggettività.

6. Quando adotta posizioni, pareri e relazioni, il gruppo di esperti cerca di raggiungere un consenso. Se non è possibile raggiungere un consenso, le decisioni sono prese a maggioranza semplice dei membri del gruppo.

Emendamento 157

Proposta di regolamento
Articolo 53 – paragrafo 1

Testo della Commissione	*Emendamento*
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.	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 ***e tengono conto delle specificità delle micro, piccole e medie imprese***.

Emendamento 158

Proposta di regolamento
Articolo 53 – paragrafo 6 – lettera a bis (nuova)

Testo della Commissione	*Emendamento*
	a bis) la violazione non è intenzionale;

Emendamento 159

Proposta di regolamento
Articolo 53 – paragrafo 6 – lettera b

Testo della Commissione	*Emendamento*
b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per una violazione analoga;	b) se ***identiche o*** altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per una violazione analoga;

Emendamento 160

Proposta di regolamento
Articolo 53 – paragrafo 6 – lettera c

Testo della Commissione	*Emendamento*
c) le dimensioni e la quota di mercato dell'operatore che ha commesso la violazione.	c) le dimensioni e la quota di mercato dell'operatore che ha commesso la violazione***, tenendo conto della portata dei rischi, delle conseguenze e delle specificità finanziarie delle micro, piccole e medie imprese***;

Emendamento 161

Proposta di regolamento
Articolo 53 – paragrafo 6 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	c bis) il successivo comportamento dell'operatore a seguito di informazioni o conoscenza della rispettiva non conformità, e anche se una volta venuto a conoscenza della rispettiva non conformità, l'operatore ha adottato tutte le opportune misure correttive nonché ragionevolmente necessarie per evitare o minimizzare potenziali conseguenze negative.

Emendamento 162

Proposta di regolamento
Capo VII bis (nuovo)

Testo della Commissione	*Emendamento*
	MISURE A SOSTEGNO DELL'INNOVAZIONE

Emendamento 163

Proposta di regolamento
Articolo 53 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 53 bis
	Spazi di sperimentazione normativa
	La Commissione e l'ENISA possono istituire uno spazio europeo di sperimentazione normativa con la partecipazione volontaria dei fabbricanti di prodotti con elementi digitali al fine di:
	a) fornire un ambiente controllato che faciliti lo sviluppo, le prove e la convalida della progettazione, dello sviluppo e della produzione di prodotti con elementi digitali, prima della loro immissione sul mercato o della loro messa in servizio in base a un piano specifico;

	b) fornire un supporto pratico agli operatori economici, anche mediante orientamenti e buone pratiche per conformarsi ai requisiti essenziali di cui all'allegato I;
	c) contribuire all'apprendimento normativo basato su dati concreti.

Emendamento 164

Proposta di regolamento
Articolo 54 – titolo

Testo della Commissione	*Emendamento*
Modifica del regolamento (UE) 2019/1020	***Modifiche*** del regolamento (UE) 2019/1020 ***e della direttiva 2020/1828/CE***

Emendamento 165

Proposta di regolamento
Articolo 54 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. Nell'allegato I della direttiva 2020/1828/CE è aggiunto il punto seguente:
	"67. [regolamento XXX][legge sulla ciberresilienza]".

Emendamento 166

Proposta di regolamento
Articolo 54 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 54 bis
	Regolamento delegato (UE) 2022/30
	Il presente regolamento è concepito in modo tale che tutti i prodotti coperti dai requisiti essenziali di cui all'articolo 3, paragrafo 3, lettere d), e) e f) della

	direttiva 2014/53/UE descritti nel regolamento delegato (UE) 2022/30 sono conformi al presente regolamento. Ai fini della certezza del diritto, il regolamento delegato (UE) 2022/30 sarà abrogato all'entrata in vigore del presente regolamento.

Emendamento 167

Proposta di regolamento
Articolo 57 – comma 2

Testo della Commissione	*Emendamento*
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].	Esso si applica a partire dal [***36*** mesi dopo la data della sua entrata in vigore]. ***Per quanto riguarda i prodotti con elementi critici, i capi II, III, V e VII*** si ***applicano non prima di*** [***20*** mesi dopo la data di ***pubblicazione delle norme armonizzate sviluppate nell'ambito dei requisiti di normazione ai fini*** del presente regolamento]. ***Entro 6 mesi dopo la data di entrata in vigore del presente regolamento, la Commissione pubblica orientamenti su come applicare i requisiti del presente regolamento ai prodotti non tangibili.***

Emendamento 168

Proposta di regolamento
Allegato I – parte 1 – punto 3 – parte introduttiva

Testo della Commissione	*Emendamento*
(3) Sulla base della valutazione dei rischi di cui all'articolo 10, paragrafo 2, e ove applicabile, i prodotti con elementi digitali:	(3) Sulla base della valutazione dei rischi di ***cibersicurezza di*** cui all'articolo 10, paragrafo 2, e ove applicabile, i prodotti con elementi digitali:

Emendamento 169

Proposta di regolamento
Allegato I – parte 1 – punto 3 – lettera -a (nuova)

Testo della Commissione	*Emendamento*
	-a) sono immessi sul mercato senza alcuna vulnerabilità sfruttabile nota nei confronti di un dispositivo o una rete esterni;

Emendamento 170

Proposta di regolamento
Allegato I – parte 1 – punto 3 – lettera a

Testo della Commissione	*Emendamento*
a) sono forniti con una configurazione sicura per impostazione predefinita***, con la possibilità di ripristinare il prodotto allo stato originale***;	a) sono forniti con una configurazione sicura per impostazione predefinita;

Emendamento 171

Proposta di regolamento
Allegato I – parte 1 – punto 3 – lettera c

Testo della Commissione	*Emendamento*
c) proteggono la riservatezza dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, ad esempio ***criptando i*** pertinenti dati a riposo o in transito mediante meccanismi all'avanguardia;	c) proteggono la riservatezza dei dati personali o di altro tipo conservati, trasmessi o altrimenti trattati, ad esempio ***attraverso crittografia, tokenizzazione, controlli di compensazione o altra protezione adeguata dei*** pertinenti dati a riposo o in transito mediante meccanismi all'avanguardia;

Emendamento 172

Proposta di regolamento
Allegato I – parte 1 – punto 3 – lettera d

Testo della Commissione	*Emendamento*
d) proteggono l'integrità dei dati	d) proteggono l'integrità dei dati

personali o di altro tipo conservati, trasmessi o altrimenti trattati, dei comandi, dei programmi e della configurazione da qualsiasi manipolazione o modifica non autorizzata da parte dell'utilizzatore, e segnalano le corruzioni;	personali o di altro tipo conservati, trasmessi o altrimenti trattati, dei comandi, dei programmi e della configurazione da qualsiasi manipolazione o modifica non autorizzata da parte dell'utilizzatore, e segnalano le corruzioni ***o i potenziali accessi non autorizzati***;

Emendamento 173

Proposta di regolamento
Allegato I – parte 1 – punto 3 – lettera f

Testo della Commissione	*Emendamento*
f) proteggono la disponibilità delle funzioni essenziali, comprese la resilienza e l'attenuazione degli attacchi di negazione del servizio (denial of service);	f) proteggono la disponibilità delle funzioni essenziali ***e di base***, comprese la resilienza e l'attenuazione degli attacchi di negazione del servizio (denial of service);

Emendamento 174

Proposta di regolamento
Allegato I – parte 1 – punto 3 – lettera i

Testo della Commissione	*Emendamento*
i) sono progettati, sviluppati e prodotti per ridurre l'impatto degli incidenti utilizzando meccanismi e tecniche di attenuazione dello sfruttamento adeguati;	i) sono progettati, sviluppati e prodotti per ridurre l'impatto degli incidenti ***significativi*** utilizzando meccanismi e tecniche di attenuazione dello sfruttamento adeguati;

Emendamento 175

Proposta di regolamento
Allegato I – parte 1 – punto 3 – lettera j

Testo della Commissione	*Emendamento*
j) forniscono informazioni sulla sicurezza ***registrando*** e/o ***monitorando le*** attività interne pertinenti, compresi l'accesso a dati, servizi o funzioni o la modifica degli stessi;	j) forniscono informazioni sulla sicurezza***, su richiesta dell'utente, tramite funzionalità di registrazione*** e/o ***monitoraggio, a livello locale e di dispositivo, delle*** attività interne pertinenti, compresi l'accesso a dati, servizi o funzioni

o la modifica degli stessi;

Emendamento 176

Proposta di regolamento
Allegato I – parte 1 – punto 3 – lettera k

Testo della Commissione	*Emendamento*
k) garantiscono che le vulnerabilità possano essere affrontate tramite aggiornamenti di sicurezza, compresi, se del caso, gli aggiornamenti automatici e la notifica agli utilizzatori degli aggiornamenti disponibili.	k) garantiscono che le vulnerabilità possano essere affrontate tramite aggiornamenti di sicurezza, ***separati dagli aggiornamenti delle funzionalità,*** compresi, se del caso, gli aggiornamenti automatici e la notifica agli utilizzatori degli aggiornamenti disponibili;

Emendamento 177

Proposta di regolamento
Allegato I – parte 1 – punto 3 – lettera k bis (nuova)

Testo della Commissione	*Emendamento*
	k bis) sono progettati, sviluppati e prodotti in modo da consentirne l'interruzione sicura e il potenziale riciclaggio al termine del ciclo di vita, anche permettendo agli utilizzatori di ritirare ed eliminare in modo sicuro tutti i dati in modo permanente.

Emendamento 178

Proposta di regolamento
Allegato I – parte 2 – punto 2

Testo della Commissione	*Emendamento*
(2) in relazione ai rischi posti dai prodotti con elementi digitali, affrontano e correggono tempestivamente le vulnerabilità, anche fornendo aggiornamenti di sicurezza;	(2) in relazione ai rischi posti dai prodotti con elementi digitali, affrontano e correggono tempestivamente le vulnerabilità ***critiche e di elevata gravità***, anche fornendo aggiornamenti di sicurezza ***o documentano i motivi della mancata***

correzione della vulnerabilità;

Emendamento 179

Proposta di regolamento
Allegato I – parte 2 – punto 4

Testo della Commissione	*Emendamento*
(4) una volta reso disponibile un aggiornamento di sicurezza, divulgano pubblicamente informazioni sulle vulnerabilità risolte, compresi una descrizione delle vulnerabilità, informazioni che consentano agli utilizzatori di identificare il prodotto con elementi digitali interessato, l'impatto delle vulnerabilità, la loro gravità e informazioni che aiutino gli utilizzatori a correggere le vulnerabilità;	(4) una volta reso disponibile un aggiornamento di sicurezza, divulgano pubblicamente ***o sulla base delle migliori pratiche del settore*** informazioni sulle vulnerabilità ***note*** risolte, compresi una descrizione delle vulnerabilità, informazioni che consentano agli utilizzatori di identificare il prodotto con elementi digitali interessato, l'impatto delle vulnerabilità, la loro gravità e informazioni ***chiare e accessibili*** che aiutino gli utilizzatori a correggere le vulnerabilità;

Emendamento 180

Proposta di regolamento
Allegato I – parte 2 – punto 4 bis (nuova)

Testo della Commissione	*Emendamento*
	4 bis) provvedono affinché le informazioni relative alle correzioni e alle vulnerabilità siano condivise e divulgate in modo controllato, rispettando i principi della riduzione dei danni e del segreto commerciale attraverso la divulgazione responsabile delle vulnerabilità ai soggetti che possono agire per attenuare le vulnerabilità, e non siano rese disponibili al pubblico per evitare il rischio di informare inavvertitamente potenziali aggressori;

Emendamento 181

Proposta di regolamento
Allegato I – parte 2 – punto 7

Testo della Commissione	*Emendamento*
(7) prevedono meccanismi per distribuire in modo sicuro gli aggiornamenti dei prodotti con elementi digitali, per garantire che le vulnerabilità sfruttabili siano corrette o attenuate in modo tempestivo;	(7) prevedono meccanismi per distribuire in modo sicuro gli aggiornamenti ***di sicurezza*** dei prodotti con elementi digitali, per garantire che le vulnerabilità sfruttabili siano corrette o attenuate in modo tempestivo;

Emendamento 182

Proposta di regolamento
Allegato I – parte 2 – punto 8

Testo della Commissione	*Emendamento*
(8) garantiscono che, qualora ***disponibili, siano diffusi tempestivamente e gratuitamente patch o aggiornamenti di sicurezza*** per risolvere i problemi di sicurezza individuati, accompagnati da messaggi di avviso che forniscano agli utilizzatori le informazioni pertinenti, comprese le potenziali misure da adottare.	(8) garantiscono che, qualora ***patch o aggiornamenti di sicurezza possano essere ragionevolmente resi disponibili*** per risolvere i problemi di sicurezza individuati***, vi sia un mezzo che consenta agli utenti di ottenerli e diffonderli tempestivamente e gratuitamente o a un costo trasparente e non discriminatorio***, accompagnati da messaggi di avviso che forniscano agli utilizzatori le informazioni pertinenti, comprese le potenziali misure da adottare.

Emendamento 183

Proposta di regolamento
Allegato II – paragrafo 2

Testo della Commissione	*Emendamento*
2. il punto di contatto dove è possibile segnalare e ricevere informazioni sulle vulnerabilità di cibersicurezza del prodotto;	2. il punto di contatto ***unico*** dove è possibile segnalare e ricevere informazioni sulle vulnerabilità di cibersicurezza del prodotto;

Emendamento 184

Proposta di regolamento
Allegato II – paragrafo 5

Testo della Commissione	*Emendamento*
5. qualsiasi circostanza nota o prevedibile connessa all'uso del prodotto con elementi digitali in conformità alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, che possa comportare rischi di cibersicurezza significativi;	***soppresso***

Emendamento 185

Proposta di regolamento
Allegato II – paragrafo 6

Testo della Commissione	*Emendamento*
6. se e, ove applicabile, dove è possibile accedere alla distinta base del software;	6. se e, ove applicabile, dove è possibile ***per le autorità competenti*** accedere alla distinta base del software;

Emendamento 186

Proposta di regolamento
Allegato II – paragrafo 8

Testo della Commissione	*Emendamento*
8. il tipo di assistenza tecnica di sicurezza offerta dal fabbricante e fino a quando essa sarà fornita***, come minimo fino a quando gli utilizzatori possono aspettarsi di ricevere gli aggiornamenti di sicurezza***;	8. il tipo di assistenza tecnica di sicurezza offerta dal fabbricante e fino a quando essa sarà fornita;

Emendamento 187

Proposta di regolamento
Allegato II – paragrafo 8 bis (nuovo)

Testo della Commissione	*Emendamento*
	8 bis. la data di fine della durata prevista del prodotto, chiaramente indicata, se del caso, sull'imballaggio del prodotto, fino a

	quando il fabbricante garantisce la gestione efficace delle vulnerabilità e la fornitura di aggiornamenti di sicurezza;

Emendamento 188

Proposta di regolamento
Allegato II – paragrafo 9 – lettera a

Testo della Commissione	*Emendamento*
a) le misure necessarie durante la prima messa in servizio e per tutta la durata del prodotto per garantirne l'uso sicuro;	***soppresso***

Emendamento 189

Proposta di regolamento
Allegato II – paragrafo 9 – lettera b

Testo della Commissione	*Emendamento*
b) in che modo le modifiche del prodotto possono influire sulla sicurezza dei dati;	***soppresso***

Emendamento 190

Proposta di regolamento
Allegato II – paragrafo 9 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	c bis) la durata prevista del prodotto e fino a quando il fabbricante garantisce la gestione efficace delle vulnerabilità e la fornitura di aggiornamenti di sicurezza;

Emendamento 191

Proposta di regolamento
Allegato II – paragrafo 9 – lettera d

Testo della Commissione	*Emendamento*
d) lo smantellamento sicuro del prodotto, comprese le informazioni sulle modalità di eliminazione sicura dei dati degli utilizzatori.	***soppresso***

Emendamento 192

Proposta di regolamento
Allegato III – Classe I – paragrafo 3 bis (nuovo)

Testo della Commissione	*Emendamento*
	3 bis. piattaforme di autenticazione, autorizzazione e accounting (AAA);

Emendamento 193

Proposta di regolamento
Allegato III – Classe I – paragrafo 15

Testo della Commissione	*Emendamento*
15. interfacce di rete fisiche;	15. interfacce di rete fisiche ***e virtuali***;

Emendamento 194

Proposta di regolamento
Allegato III – Classe I – paragrafo 18

Testo della Commissione	*Emendamento*
18. router, modem per la connessione a internet e switch non compresi nella classe II;	***soppresso***

Emendamento 195

Proposta di regolamento
Allegato III – Classe I – paragrafo 23

Testo della Commissione	*Emendamento*
23. ***internet*** delle cose ***industriale*** non ***rientrante*** nella classe II.	23. ***prodotti industriali con elementi digitali che possono essere considerati parte dell'internet*** delle cose non ***rientranti*** nella classe II.

Emendamento 196

Proposta di regolamento
Allegato III – Classe II – paragrafo 4

Testo della Commissione	*Emendamento*
4. firewall, sistemi di rilevamento e/o prevenzione delle intrusioni destinati all'uso industriale;	4. firewall, ***gateway di sicurezza,*** sistemi di rilevamento e/o prevenzione delle intrusioni destinati all'uso industriale;

Emendamento 197

Proposta di regolamento
Allegato III – Classe II – paragrafo 7

Testo della Commissione	*Emendamento*
7. router, modem per la connessione a internet e ***switch*** per ***uso industriale***;	7. router, modem per la connessione a internet***, switch*** e ***altri nodi di rete necessari*** per ***la fornitura del servizio di connettività***;

Emendamento 198

Proposta di regolamento
Allegato IV bis (nuovo)

Testo della Commissione	*Emendamento*
	Allegato IV bis
	DICHIARAZIONE UE DI INCORPORAZIONE PER PRODOTTI CON ELEMENTI DIGITALI PAZIALMENTE COMPLETATI
	La dichiarazione UE di incorporazione per prodotti con elementi digitali

	parzialmente completati di cui all'articolo 20 bis contiene tutte le informazioni seguenti:
	1. nome e tipo e qualsiasi altra informazione che consenta l'identificazione univoca del prodotto con elementi digitali parzialmente completato;
	2. oggetto della dichiarazione (identificazione prodotto parzialmente completato che ne consenta la tracciabilità. Può comprendere, se del caso, una fotografia);
	3. un'attestazione secondo la quale il prodotto parzialmente completato di cui sopra è conforme alla pertinente normativa di armonizzazione dell'Unione;
	4. i riferimenti ai pertinenti atti dell'Unione in questione, compresi i riferimenti alla loro pubblicazione;
	5. informazioni supplementari:
	Firmato a nome e per conto di:
	……
	(luogo e data del rilascio):
	(nome e cognome, funzione) (firma)

Emendamento 199

Proposta di regolamento
Allegato V – paragrafo 1 – lettera a

Testo della Commissione	*Emendamento*
a) la finalità prevista;	***soppresso***

Emendamento 200

Proposta di regolamento
Allegato V – paragrafo 2

Testo della Commissione	*Emendamento*
2. una descrizione della progettazione, dello sviluppo e della	***soppresso***

produzione del prodotto e dei processi di gestione delle vulnerabilità, tra cui:

a) informazioni complete sulla progettazione e sullo sviluppo del prodotto con elementi digitali, compresi, se del caso, disegni e schemi e/o una descrizione dell'architettura del sistema che spieghi in che modo i componenti software si basano l'uno sull'altro o si alimentano reciprocamente e si integrano nel processo complessivo;

b) informazioni complete e specifiche sui processi di gestione delle vulnerabilità messi in atto dal fabbricante, tra cui la distinta base del software, la politica di gestione della divulgazione coordinata delle vulnerabilità, la prova della fornitura di un indirizzo di contatto per la segnalazione delle vulnerabilità e una descrizione delle soluzioni tecniche scelte per la distribuzione sicura degli aggiornamenti;

c) informazioni complete e specifiche relative ai processi di produzione e monitoraggio del prodotto con elementi digitali e alla convalida di tali processi;

Emendamento 201

Proposta di regolamento
Allegato V – paragrafo 3

Testo della Commissione	*Emendamento*
3. una valutazione dei rischi di cibersicurezza a fronte dei quali il prodotto con elementi digitali è progettato, sviluppato, prodotto, consegnato e sottoposto a manutenzione, come stabilito all'articolo 10 del presente regolamento;	3. ***una dichiarazione o una sintesi dei rischi di cibersicurezza a fronte dei quali il prodotto con elementi digitali è progettato, sviluppato, prodotto, consegnato e sottoposto a manutenzione, come stabilito all'articolo 10 del presente regolamento e, a seguito di una richiesta motivata di un'autorità di vigilanza del mercato, a condizione che sia necessaria affinché tale autorità possa verificare la conformità ai requisiti essenziali di cui all'allegato I,*** una valutazione ***dettagliata*** dei rischi di cibersicurezza a fronte dei

quali il prodotto con elementi digitali è progettato, sviluppato, prodotto, consegnato e sottoposto a manutenzione, come stabilito all'articolo 10 del presente regolamento;

ALLEGATO: ELENCO DELLE ENTITÀ O DELLE PERSONE DA CUI IL RELATORE PER PARERE HA RICEVUTO CONTRIBUTI

L'elenco in appresso è compilato su base puramente volontaria, sotto l'esclusiva responsabilità del relatore per parere. Nel corso dell'elaborazione del parere, il relatore per parere ha ricevuto contributi dalle seguenti entità o persone:

Entity and/or person
Apple
BDI Federation of German Industries
BEUC
BSA The Software Alliance
Confederation of Danish Industries
Digital Europe
ETNO
Kaspersky
Microsoft
Samsung
TIC Council
Xiaomi

PROCEDURA DELLA COMMISSIONE COMPETENTE PER PARERE

Titolo	Requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020
Riferimenti	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)
Commissione competente per il merito Annuncio in Aula	ITRE 9.11.2022
Parere espresso da Annuncio in Aula	IMCO 9.11.2022
Commissioni associate - annuncio in aula	20.4.2023
Relatrice per parere: Nomina	Morten Løkkegaard 16.12.2022
Esame in commissione	2.3.2023 25.4.2023 23.5.2023
Approvazione	29.6.2023
Esito della votazione finale	+: 41 –: 1 0: 0
Membri titolari presenti al momento della votazione finale	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Biljana Borzan, Vlad-Marius Botoş, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Alexandra Geese, Maria Grapini, Svenja Hahn, Krzysztof Hetman, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Kateřina Konečná, Andrey Kovatchev, Maria-Manuel Leitão-Marques, Antonius Manders, Beata Mazurek, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, René Repasi, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann
Supplenti presenti al momento della votazione finale	Marco Campomenosi, Maria da Graça Carvalho, Geoffroy Didier, Francisco Guerreiro, Tsvetelina Penkova, Catharina Rinzema, Kosma Złotowski
Supplenti (art. 209, par. 7) presenti al momento della votazione finale	Asger Christensen, Nicolás González Casares, Grzegorz Tobiszowski

VOTAZIONE FINALE PER APPELLO NOMINALE IN SEDE DI COMMISSIONE COMPETENTE PER PARERE

41	+
ECR	Beata Mazurek, Grzegorz Tobiszowski, Kosma Złotowski
ID	Alessandra Basso, Marco Campomenosi, Virginie Joron
NI	Miroslav Radačovský
PPE	Pablo Arias Echeverría, Maria da Graça Carvalho, Deirdre Clune, Geoffroy Didier, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Asger Christensen, Svenja Hahn, Catharina Rinzema
S&D	Alex Agius Saliba, Biljana Borzan, Nicolás González Casares, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Tsvetelina Penkova, René Repasi, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Francisco Guerreiro, Kim Van Sparrentak

1	-
ECR	Eugen Jurzyca

0	0

Significato dei simboli utilizzati:
+ : favorevoli
- : contrari
0 : astenuti

PROCEDURA DELLA COMMISSIONE COMPETENTE PER IL MERITO

Titolo	Requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e modifica del regolamento (UE) 2019/1020
Riferimenti	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)
Presentazione della proposta al PE	15.9.2022
Commissione competente per il merito Annuncio in Aula	ITRE 9.11.2022
Commissioni competenti per parere Annuncio in Aula	IMCO LIBE 9.11.2022 9.11.2022
Commissioni associate Annuncio in Aula	LIBE IMCO 20.4.2023 20.4.2023
Relatori Nomina	Nicola Danti 26.10.2022
Esame in commissione	25.4.2023
Approvazione	19.7.2023
Esito della votazione finale	+: 61 –: 1 0: 10
Membri titolari presenti al momento della votazione finale	Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Vasile Blaga, Michael Bloss, Paolo Borchia, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Ignazio Corrao, Beatrice Covassi, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Jens Geier, Nicolás González Casares, Christophe Grudler, Henrike Hahn, Robert Hajšel, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Zdzisław Krasnodębski, Andrius Kubilius, Thierry Mariani, Marisa Matias, Marina Mesure, Dan Nica, Niklas Nienass, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Maria Spyraki, Grzegorz Tobiszowski, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho
Supplenti presenti al momento della votazione finale	Damian Boeselager, Franc Bogovič, Francesca Donato, Matthias Ecke, Ladislav Ilčić, Elena Lizzi, Dace Melbārde, Jutta Paulus, Massimiliano Salini, Jordi Solé, Susana Solís Pérez, Ivan Štefanec, Nils Torvalds, Emma Wiesner
Supplenti (art. 209, par. 7) presenti al momento della votazione finale	Rosanna Conte, Arnaud Danjean, César Luena, Nicola Procaccini, Elżbieta Rafalska, Antonio Maria Rinaldi, Daniela Rondinelli, Nacho Sánchez Amor, Edina Tóth
Deposito	27.7.2023

VOTAZIONE FINALE PER APPELLO NOMINALE IN SEDE DI COMMISSIONE COMPETENTE PER IL MERITO

61	+
ECR	Ladislav Ilčić, Zdzisław Krasnodębski, Nicola Procaccini, Elżbieta Rafalska, Grzegorz Tobiszowski
NI	Francesca Donato, Edina Tóth
PPE	François-Xavier Bellamy, Hildegard Bentele, Vasile Blaga, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Arnaud Danjean, Christian Ehler, Seán Kelly, Andrius Kubilius, Dace Melbārde, Markus Pieper, Massimiliano Salini, Maria Spyraki, Ivan Štefanec, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Christophe Grudler, Ivars Ijabs, Mauri Pekkarinen, Morten Petersen, Susana Solís Pérez, Nils Torvalds, Emma Wiesner
S&D	Beatrice Covassi, Matthias Ecke, Niels Fuglsang, Jens Geier, Nicolás González Casares, Robert Hajšel, Ivo Hristov, Romana Jerković, César Luena, Dan Nica, Tsvetelina Penkova, Daniela Rondinelli, Nacho Sánchez Amor, Patrizia Toia, Carlos Zorrinho
Verts/ALE	Michael Bloss, Damian Boeselager, Ignazio Corrao, Henrike Hahn, Niklas Nienass, Ville Niinistö, Jutta Paulus, Manuela Ripa, Jordi Solé

1	-
The Left	Marina Mesure

10	0
ECR	Johan Nissinen, Robert Roos
ID	Paolo Borchia, Rosanna Conte, Marie Dauchy, Elena Lizzi, Thierry Mariani, Antonio Maria Rinaldi
PPE	Sara Skyttedal
The Left	Marisa Matias

Significato dei simboli utilizzati:
+ : favorevoli
- : contrari
0 : astenuti