



---

*Commissione per il mercato interno e la protezione dei consumatori*

---

**2022/0272(COD)**

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

PA\_Legam

## 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 cibersecurity dell'Unione europea. Consapevole del fatto che, per definizione, la cibersecurity 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 cibersecurity 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 cibersecurity 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 cibersecurity 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 cibersecurity nella nostra Unione. Con gli emendamenti suggeriti, il relatore ha cercato di trovare il giusto equilibrio tra la garanzia di un maggiore livello di cibersecurity 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*

(1) Occorre migliorare il funzionamento del mercato interno, definendo un quadro giuridico uniforme per i requisiti essenziali di cibersecurity 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 cibersecurity 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 cibersecurity adeguate o di utilizzarli in modo sicuro.

##### *Emendamento*

(1) Occorre migliorare il funzionamento del mercato interno **e garantire al tempo stesso un livello elevato di protezione dei consumatori e di cibersecurity**, definendo un quadro giuridico uniforme per i requisiti essenziali di cibersecurity 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 cibersecurity 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 cibersecurity adeguate o di utilizzarli in modo sicuro.

### Emendamento 2

#### Proposta di regolamento Considerando 7

##### *Testo della Commissione*

(7) In determinate condizioni tutti i prodotti con elementi digitali integrati in

##### *Emendamento*

(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.

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 **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 cibersecurity 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 cibersecurity 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

(9) Il presente regolamento garantisce un livello elevato di cibersecurity 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 cibersecurity 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.

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*

(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.

#### *Emendamento*

(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*

(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

#### *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 [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.

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 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*

(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

#### *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, **quando** la Commissione abroga il regolamento delegato (UE) 2022/30, con la conseguenza che esso cessa di applicarsi a determinati

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.

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.

## **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*

(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

#### *Emendamento*

(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, **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

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.

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.

## **Emendamento 11**

### **Proposta di regolamento Considerando 20**

#### *Testo della Commissione*

(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.

#### *Emendamento*

(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*

(22) Per garantire che i prodotti con

#### *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 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.

## **Emendamento 13**

### **Proposta di regolamento**

#### **Considerando 23**

##### *Testo della Commissione*

(23) In linea con la nozione generalmente riconosciuta di modifica sostanziale dei prodotti disciplinati dalla normativa di armonizzazione dell'Unione, ogniqualvolta intervenga una modifica

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, ***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*

(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.

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. *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*

(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.

#### *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, ***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*

(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.

### *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 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*

(29) I prodotti con elementi digitali classificati come sistemi di IA ad alto rischio conformemente all'articolo 6 del regolamento<sup>27</sup> [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

#### *Emendamento*

(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<sup>27</sup> [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

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'IA], 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].***

---

<sup>27</sup> Regolamento [regolamento sull'IA].

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 ***[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.***

---

<sup>27</sup> Regolamento [regolamento sull'IA].

## Emendamento 18

### Proposta di regolamento Considerando 32

*Testo della Commissione*

(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.

*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 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*

(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.

#### *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, **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

(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

rapidamente agli incidenti che hanno un impatto sulla sicurezza dei loro prodotti con elementi digitali, i fabbricanti dovrebbero inoltre informare gli utilizzatori di tali incidenti e, se del caso, di **eventuali misure correttive** che gli utilizzatori potrebbero adottare per attenuarne l'impatto, ad esempio attraverso la pubblicazione di informazioni pertinenti sui propri siti web o il contatto diretto, qualora il fabbricante sia in grado di contattare gli utilizzatori e ciò sia giustificato dai rischi.

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 **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 cibersecurity 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*

(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<sup>29</sup>. Il regolamento (UE) n. 1025/2012 prevede una procedura di obiezione a norme armonizzate che non soddisfano completamente i requisiti del presente regolamento.

---

<sup>29</sup> 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*

(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<sup>29</sup>. 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.***

---

<sup>29</sup> 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*

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

*Emendamento*

(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) 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*

(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

*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<sup>30</sup>. 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.

---

<sup>30</sup> 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*

(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

che disciplinano la marcatura CE sono indicati nel regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio<sup>30</sup>. 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. ***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.***

---

<sup>30</sup> 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*

(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

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 cibersecurity a norma del regolamento (UE) 2019/881 che sono stati identificati dalla Commissione in un atto di esecuzione. Se non applica tali norme armonizzate, **specifiche comuni** o sistemi di certificazione della cibersecurity, 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 cibersecurity 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 cibersecurity ancora maggiore legato all'uso di prodotti classificati come prodotti critici di classe II, la valutazione della conformità dovrebbe sempre coinvolgere terzi.

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 cibersecurity a norma del regolamento (UE) 2019/881 che sono stati identificati dalla Commissione in un atto di esecuzione. Se non applica tali norme armonizzate o sistemi di certificazione della cibersecurity, 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 cibersecurity 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 cibersecurity 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*

(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 cibersecurity 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

#### *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 **8** della direttiva **2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersecurity 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 cibersecurity 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

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.

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**

(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

(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 **(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.

considerazione l'adozione di proposte per rivedere la corrispondente normativa dell'Unione.

### **Emendamento 33**

#### **Proposta di regolamento Considerando 59**

##### *Testo della Commissione*

(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

##### *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 **(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

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.

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*

(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

#### *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 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<sup>33</sup>. 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.

---

<sup>33</sup> GU L 123 del 12.5.2016, pag. 1.

esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016<sup>33</sup>. 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.

---

<sup>33</sup> GU L 123 del 12.5.2016, pag. 1.

## Emendamento 35

### Proposta di regolamento Considerando 63

#### *Testo della Commissione*

(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 cibersecurity 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

#### *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 **sulla base delle migliori pratiche del settore**, specificare i sistemi europei di certificazione della cibersecurity 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

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<sup>34</sup>.

---

<sup>34</sup> 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).

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<sup>34</sup>.

---

<sup>34</sup> 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*

(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.***

## Emendamento 37

### Proposta di regolamento Articolo 1 – parte introduttiva

#### *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 [36 mesi] dopo la sua entrata in vigore

*Testo della Commissione*

Il presente regolamento stabilisce:

*Emendamento*

***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 cibersecurity.***

Il presente regolamento stabilisce ***norme armonizzate per quanto riguarda:***

**Emendamento 38**

**Proposta di regolamento  
Articolo 1 – lettera a**

*Testo della Commissione*

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

*Emendamento*

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

**Emendamento 39**

**Proposta di regolamento  
Articolo 1 – lettera d**

*Testo della Commissione*

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

*Emendamento*

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*

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

*Emendamento*

1. Il presente regolamento si applica ai prodotti con elementi digitali ***immessi sul mercato*** il cui uso previsto o ragionevolmente prevedibile include una

diretta o indiretta a un dispositivo o a una rete.

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*

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;

#### *Emendamento*

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*

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.

#### *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 ***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*

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.

#### *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, ***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*

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

#### *Emendamento*

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 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*

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

*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, **ricevano i necessari aggiornamenti di sicurezza**, e

**Emendamento 60**

**Proposta di regolamento  
Articolo 6 – paragrafo 1**

*Testo della Commissione*

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.

*Emendamento*

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*

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)];

*Emendamento*

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*

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

*Emendamento*

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*

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

*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. **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*

5. Alla Commissione è conferito il potere di adottare atti delegati

*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:

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*

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

##### *Emendamento*

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

regolamento.

dalla dichiarazione di conformità UE rilasciata a norma del presente regolamento.

## **Emendamento 66**

### **Proposta di regolamento Articolo 8 – paragrafo 2**

#### *Testo della Commissione*

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

#### *Emendamento*

2. Per quanto riguarda i prodotti e i requisiti di cibersecurity 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.

## **Emendamento 67**

### **Proposta di regolamento Articolo 8 – paragrafo 3**

#### *Testo della Commissione*

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),***

#### *Emendamento*

***soppresso***

*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.*

## **Emendamento 68**

### **Proposta di regolamento Articolo 9**

#### *Testo della Commissione*

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.

#### *Emendamento*

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)

***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*

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 cibersecurity 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.

*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 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 cibersecurity 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 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.

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.

**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 venuta a conoscenza, qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto

1. Il fabbricante notifica all'ENISA, senza indebito ritardo e comunque entro **48** ore dal momento in cui ne è venuta a conoscenza, **mediante una segnalazione preventiva**, qualsiasi vulnerabilità

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.***

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

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. ***II***

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.

***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*

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.

*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 **significativi** e delle crisi di cibersicurezza su vasta scala a livello operativo.

**Emendamento 85**

**Proposta di regolamento**  
**Articolo 11 – paragrafo 4**

*Testo della Commissione*

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.

*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 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*

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.

#### *Emendamento*

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*

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

#### *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 ***14*** della direttiva ***(UE) 2022/2555***. La prima relazione di questo tipo è presentata entro 24 mesi dall'inizio dell'applicazione degli

dell'applicazione degli obblighi di cui ai paragrafi 1 e 2.

obblighi di cui ai paragrafi 1 e 2.

## Emendamento 89

### Proposta di regolamento Articolo 11 – paragrafo 7

#### *Testo della Commissione*

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.

#### *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, ***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*

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:

#### *Emendamento*

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)

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

## Emendamento 92

### Proposta di regolamento

#### Articolo 12 – paragrafo 3 – lettera b

*Testo della Commissione*

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;

*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 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*

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.

*Emendamento*

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)

***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*

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.

*Emendamento*

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*

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,

*Emendamento*

*(Non concerne la versione italiana)*

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.

## **Emendamento 97**

### **Proposta di regolamento**

#### **Articolo 13 – paragrafo 6 – comma 1**

##### *Testo della Commissione*

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.

##### *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. ***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*

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.

#### *Emendamento*

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 cibersecurity.***

*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*

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

#### *Emendamento*

*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:*

*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*

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.

#### *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 **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*

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.

#### *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 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*

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.

*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 ***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*

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.

*Emendamento*

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*

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

*Emendamento*

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

promuoverne l'uso. Tali atti *di esecuzione* sono adottati secondo la procedura *d'esame* di cui all'articolo 51, paragrafo 2.

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*

## **Emendamento 115**

### **Proposta di regolamento Articolo 23 – paragrafo 2**

#### *Testo della Commissione*

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**.

#### *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 **lungo**.

## **Emendamento 116**

### **Proposta di regolamento Articolo 23 – paragrafo 3**

#### *Testo della Commissione*

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.

#### *Emendamento*

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*

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 50 per integrare il presente regolamento con gli elementi da

#### *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.

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)***

## 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

5. L'autorità di notifica salvaguarda la

riservatezza delle informazioni ottenute.

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 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

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.

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*

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.

#### *Emendamento*

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*

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

#### *Emendamento*

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*

2. Le valutazioni della conformità

#### *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.

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*

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.

#### *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 **limita**, sospende o ritira il certificato.

## Emendamento 133

### Proposta di regolamento Articolo 40 – paragrafo 1

#### *Testo della Commissione*

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.

#### *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 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*

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

#### *Emendamento*

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*

3. Le autorità di vigilanza del mercato collaborano, se pertinente, con le autorità nazionali di certificazione della cibersecurity 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.

#### *Emendamento*

3. Le autorità di vigilanza del mercato collaborano, se pertinente, con le autorità nazionali di certificazione della cibersecurity 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*

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

#### *Emendamento*

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*

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.**

#### *Emendamento*

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*

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.

#### *Emendamento*

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*

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.

### *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 ***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*

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.

### *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, ***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*

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 cibersecurity 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.

### *Emendamento*

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 cibersecurity 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*

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

### *Emendamento*

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

## Emendamento 146

### Proposta di regolamento Articolo 46 – paragrafo 1

#### *Testo della Commissione*

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.

#### *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 **(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*

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.

*Emendamento*

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*

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.

*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 **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*

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

*Emendamento*

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*

1. Le autorità di vigilanza del mercato **possono stipulare accordi** con altre autorità competenti **per la realizzazione di attività congiunte** volte a garantire la cibersecurity 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 cibersecurity.

#### *Emendamento*

1. Le autorità di vigilanza del mercato **realizzano regolarmente attività congiunte** con altre autorità competenti volte a garantire la cibersecurity 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 cibersecurity. **Tali attività comprendono ispezioni sui prodotti acquistati sotto un'identità di copertura.**

## Emendamento 151

### Proposta di regolamento Articolo 48 – paragrafo 2

#### *Testo della Commissione*

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

#### *Emendamento*

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.

membri, di prodotti che rientrano 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*

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.

#### *Emendamento*

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*

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.

#### *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 **rende disponibili al pubblico, se del caso**, i risultati aggregati.

## Emendamento 154

### Proposta di regolamento Articolo 49 – paragrafo 3

#### *Testo della Commissione*

3. L'ENISA **può individuare**, nell'esecuzione dei suoi compiti, anche

#### *Emendamento*

3. L'ENISA **individua**, nell'esecuzione dei suoi compiti, anche sulla base delle

sulla base delle notifiche ricevute conformemente all'articolo 11, paragrafi 1 e 2, categorie di prodotti per le quali **possono essere** organizzate indagini a tappeto. La proposta di indagini a tappeto è sottoposta al potenziale coordinatore di cui al paragrafo 2 per essere esaminata dalle autorità di vigilanza del mercato.

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.

## **Emendamento 155**

### **Proposta di regolamento Articolo 49 – paragrafo 5**

#### *Testo della Commissione*

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.

#### *Emendamento*

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*

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,

#### *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.

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*

*Modifica* del regolamento (UE) 2019/1020

*Emendamento*

*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*

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].***

#### *Emendamento*

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*

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

#### *Emendamento*

(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*

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;

*Emendamento*

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 i potenziali accessi non autorizzati***;

**Emendamento 173**

**Proposta di regolamento**

**Allegato I – parte 1 – punto 3 – lettera f**

*Testo della Commissione*

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

*Emendamento*

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*

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

*Emendamento*

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*

j) forniscono informazioni sulla

*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;

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*

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.

##### *Emendamento*

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*

(2) in relazione ai rischi posti dai

##### *Emendamento*

(2) in relazione ai rischi posti dai

prodotti con elementi digitali, affrontano e correggono tempestivamente le vulnerabilità, anche fornendo aggiornamenti di sicurezza;

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*

(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;

#### *Emendamento*

(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*

(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;

#### *Emendamento*

(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*

(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.

#### *Emendamento*

(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*

2. il punto di contatto dove è possibile segnalare e ricevere informazioni sulle vulnerabilità di cibersicurezza del prodotto;

#### *Emendamento*

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 cibersecurity 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*

23. *internet* delle cose *industriale* non *rientrante* nella classe II.

#### *Emendamento*

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*

4. firewall, sistemi di rilevamento e/o prevenzione delle intrusioni destinati all'uso industriale;

#### *Emendamento*

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*

7. router, modem per la connessione a internet e *switch* per *uso industriale*;

#### *Emendamento*

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**

**2. una descrizione della progettazione, dello sviluppo e della produzione del prodotto e dei processi di gestione delle vulnerabilità, tra cui:**

**soppresso**

**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**

**3. una valutazione dei rischi di cibersecurity 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 cibersecurity 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:

<b>Entity and/or person</b>
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

<b>Titolo</b>	Requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020		
<b>Riferimenti</b>	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)		
<b>Commissione competente per il merito</b> Annuncio in Aula	ITRE 9.11.2022		
<b>Parere espresso da</b> Annuncio in Aula	IMCO 9.11.2022		
<b>Commissioni associate - annuncio in aula</b>	20.4.2023		
<b>Relatrice per parere:</b> Nomina	Morten Løkkegaard 16.12.2022		
<b>Esame in commissione</b>	2.3.2023	25.4.2023	23.5.2023
<b>Approvazione</b>	29.6.2023		
<b>Esito della votazione finale</b>	+: -: 0:	41 1 0	
<b>Membri titolari presenti al momento della votazione finale</b>	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Biljana Borzan, Vlad-Marius Botoș, 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		
<b>Supplenti presenti al momento della votazione finale</b>	Marco Campomenosi, Maria da Graça Carvalho, Geoffroy Didier, Francisco Guerreiro, Tsvetelina Penkova, Catharina Rinzema, Kosma Złotowski		
<b>Supplenti (art. 209, par. 7) presenti al momento della votazione finale</b>	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 Botoș, 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