Consiglio dell'Unione europea

Bruxelles, 21 aprile 2023
(OR. en)

8511/23

Fascicolo interistituzionale: 2023/0108(COD)

CYBER 91
JAI 469
TELECOM 107
DATAPROTECT 109
MI 312
IND 180
CODEC 661

PROPOSTA

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	19 aprile 2023
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2023) 208 final
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti

Si trasmette in allegato, per le delegazioni, il documento COM(2023) 208 final.

All.: COM(2023) 208 final

COMMISSIONE
EUROPEA

Strasburgo, 18.4.2023
COM(2023) 208 final

2023/0108 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti

(Testo rilevante ai fini del SEE)

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

La presente relazione accompagna la proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2019/881[1] per quanto riguarda i servizi di sicurezza gestiti.

La modifica mirata proposta intende consentire, mediante atti di esecuzione della Commissione, l'adozione di sistemi europei di certificazione della cibersicurezza per i "servizi di sicurezza gestiti", oltre che per i prodotti relativi alle tecnologie dell'informazione ("TIC"), i servizi TIC e i processi TIC, che sono già contemplati dal regolamento sulla cibersicurezza. I servizi di sicurezza gestiti svolgono un ruolo sempre più importante nella prevenzione e attenuazione degli incidenti di cibersicurezza.

Nelle sue conclusioni del 23 maggio 2022[2] sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, il Consiglio ha invitato l'Unione e i suoi Stati membri a intensificare gli sforzi tesi ad accrescere il livello complessivo della cibersicurezza, ad esempio agevolando l'emergere di fornitori di servizi di cibersicurezza affidabili e ha sottolineato che incoraggiare lo sviluppo di tali fornitori dovrebbe essere prioritario per la politica industriale dell'Unione nel settore della cibersicurezza. Ha inoltre invitato la Commissione a proporre opzioni tese a incoraggiare l'emergere di un'industria di servizi di cibersicurezza affidabile. La certificazione dei servizi di sicurezza gestiti rappresenta un mezzo efficace per creare fiducia nella qualità di tali servizi agevolando in tal modo l'emergere di un'industria di servizi di cibersicurezza affidabile.

Nella comunicazione congiunta "La politica di ciberdifesa dell'UE" adottata dalla Commissione e dall'alto rappresentante il 10 novembre 2022[3] è stato annunciato che la Commissione vaglierà lo sviluppo di sistemi di certificazione della cibersicurezza a livello UE per l'industria della cibersicurezza e le imprese private. Anche i fornitori di servizi di sicurezza gestiti svolgeranno un ruolo importante nel contesto della riserva per la cibersicurezza a livello di UE, la cui costituzione graduale è sostenuta dal regolamento sulla cibersolidarietà, proposto contemporaneamente al presente regolamento. La riserva per la cibersicurezza a livello di UE deve essere utilizzata per sostenere azioni di risposta e ripresa immediata in caso di incidenti di cibersicurezza significativi e su vasta scala. I pertinenti servizi di cibersicurezza erogati da "fornitori di fiducia" di cui al regolamento sulla cibersolidarietà corrispondono ai "servizi di sicurezza gestiti" nella presente proposta.

Alcuni Stati membri hanno già cominciato ad adottare sistemi di certificazione per i servizi di sicurezza gestiti. Vi è pertanto un crescente rischio di frammentazione del mercato interno per quanto riguarda i servizi di sicurezza gestiti a causa delle incoerenze nei sistemi di certificazione della cibersicurezza in tutta l'Unione. La presente proposta rende possibile la creazione di sistemi europei di certificazione della cibersicurezza per questi servizi al fine di prevenire tale frammentazione.

---

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

2 9364/22.

3 JOIN(2022) 49 final.

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

La presente proposta è coerente con il regolamento sulla cibersicurezza, da essa modificato, e si fonda sulle disposizioni di tale regolamento, che sono adattate per includere anche i servizi di sicurezza gestiti. Le modifiche proposte si limitano a quanto strettamente necessario e non alterano le caratteristiche o il funzionamento del regolamento sulla cibersicurezza.

La presente proposta è inoltre coerente con la 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)[4]. I fornitori di servizi di sicurezza gestiti sono ritenuti soggetti essenziali o importanti appartenenti a un settore ad alta criticità ai sensi della direttiva (UE) 2022/2555. Nel considerando 86 della direttiva si afferma che i fornitori di servizi di sicurezza gestiti, in settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza, svolgono un ruolo particolarmente importante nell'assistere i soggetti nei loro sforzi per la prevenzione e il rilevamento degli incidenti, la risposta agli stessi o la ripresa da essi. I fornitori di servizi di sicurezza gestiti sono stati tuttavia essi stessi bersaglio di attacchi informatici e presentano un particolare rischio a causa della loro stretta integrazione nelle attività dei clienti. I soggetti essenziali e importanti ai sensi della direttiva (UE) 2022/2555 dovrebbero pertanto esercitare una maggiore diligenza nella selezione di un fornitore di servizi di sicurezza gestiti.

La presente proposta intende migliorare la qualità dei servizi di sicurezza gestiti e aumentarne la comparabilità, permettendo in tal modo ai soggetti essenziali e importanti di esercitare una maggiore diligenza nella selezione di un fornitore di servizi di sicurezza gestiti, come previsto dalla direttiva (UE) 2022/2555. Inoltre la definizione di "servizi di sicurezza gestiti" di cui alla presente proposta deriva dalla definizione di "fornitori di servizi di sicurezza gestiti" di cui alla direttiva (UE) 2022/2555, a cui è molto simile. Per tali motivi la proposta è strettamente complementare alla direttiva NIS 2.

Infine la presente proposta è complementare alla proposta di regolamento sulla cibersolidarietà, che stabilisce un processo di selezione dei fornitori al fine di costituire una riserva per la cibersicurezza a livello di UE che dovrebbe, tra l'altro, considerare se tali fornitori abbiano ottenuto una certificazione della cibersicurezza europea o nazionale. I futuri sistemi di certificazione per i servizi di sicurezza gestiti svolgeranno pertanto un ruolo significativo nell'attuazione del regolamento sulla cibersolidarietà.

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

La presente proposta non incide sulla coerenza del regolamento sulla cibersicurezza con il regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati)[5] e le sue disposizioni per quanto riguarda l'istituzione di meccanismi di certificazione nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Il regolamento sulla cibersicurezza lascia impregiudicata la certificazione delle operazioni di trattamento dei dati, anche nel caso in cui tali operazioni siano integrate nei prodotti e nei servizi, nel quadro del regolamento generale sulla protezione dei dati.

Inoltre la presente proposta non pregiudica la compatibilità del regolamento sulla cibersicurezza con il regolamento (CE) n. 765/2008 sulle norme in materia di accreditamento

[4] GU L 333 del 27.12.2022, pag. 810.
[5] GU L 119 del 4.5.2016, pag. 1.

e di vigilanza del mercato[6], in particolare per quanto concerne il quadro relativo agli organismi nazionali di accreditamento e di valutazione della conformità e le autorità nazionali di controllo della certificazione.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

• Base giuridica

La presente proposta modifica il regolamento sulla cibersicurezza, basato sull'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE). Come nel caso del regolamento sulla cibersicurezza, la presente proposta mira a evitare la frammentazione del mercato interno, in particolare rendendo possibile l'adozione di sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti. Gli Stati membri hanno cominciato ad adottare sistemi nazionali di certificazione per i servizi di sicurezza gestiti: vi è pertanto un concreto rischio di frammentazione del mercato interno per quanto riguarda tali servizi, che la presente proposta intende affrontare. L'articolo 114 TFUE è quindi la base giuridica pertinente per questa iniziativa.

• Sussidiarietà (per la competenza non esclusiva)

L'obiettivo di rendere possibile l'adozione di sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti e di evitare la frammentazione del mercato interno non può essere conseguito a livello nazionale, ma solo a livello di Unione. Inoltre i servizi di sicurezza gestiti, oggetto della modifica proposta, sono offerti da fornitori che sono attivi in tutta l'Unione, così come i loro maggiori clienti potenziali. Un intervento a livello di Unione è pertanto necessario e più efficace rispetto a un'azione a livello nazionale.

• Proporzionalità

La proposta è una modifica mirata del regolamento sulla cibersicurezza ed è limitata a quanto strettamente necessario per conseguire il suo obiettivo, vale a dire rendere possibile l'adozione di sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti, oltre che per i prodotti TIC, i servizi TIC e i processi TIC. Le modifiche proposte adeguano in particolare l'ambito di applicazione del quadro europeo di certificazione della cibersicurezza per includere i "servizi di sicurezza gestiti", introducono una definizione di tali servizi in linea con la direttiva NIS 2 e modificano gli obiettivi di sicurezza della certificazione europea della cibersicurezza al fine di adattarla ai "servizi di sicurezza gestiti". Le altre modifiche sono di natura tecnica e sono intese a garantire che i pertinenti articoli si applichino anche ai "servizi di sicurezza gestiti". L'iniziativa proposta è pertanto proporzionata all'obiettivo.

• Scelta dell'atto giuridico

Poiché la proposta modifica il regolamento (UE) 2019/881, lo strumento giuridico appropriato è un regolamento.

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

• Valutazioni ex post/Vaglio di adeguatezza della legislazione vigente

Non pertinente.

[6] GU L 218 del 13.8.2008, pag. 30.

- **Consultazioni dei portatori di interessi**

Sono state effettuate consultazioni mirate con gli Stati membri e l'ENISA. Nel contesto di tali consultazioni gli Stati membri hanno descritto le attività attualmente svolte e illustrato le opinioni formulate riguardo alla certificazione dei servizi di sicurezza gestiti. L'ENISA ha esposto le proprie opinioni e l'esito delle discussioni tenutesi con gli Stati membri e i portatori di interessi. Le osservazioni e le informazioni ricevute dagli Stati membri e dall'ENISA hanno contribuito all'elaborazione della presente proposta.

- **Assunzione e uso di perizie**

Non pertinente.

- **Valutazione d'impatto**

È stata richiesta una deroga alla necessità di una valutazione d'impatto poiché la proposta è una modifica molto limitata e mirata del regolamento sulla cibersicurezza. Tale modifica autorizzerebbe la Commissione ad adottare, mediante atti di esecuzione, sistemi di certificazione per i "servizi di sicurezza gestiti", oltre che per i prodotti TIC, i servizi TIC e i processi TIC, che sono già contemplati dal regolamento, ma avrebbe effetto solo in seguito all'adozione di tali sistemi di certificazione, in una fase successiva. Inoltre la modifica non inciderebbe sul carattere volontario dei sistemi di certificazione.

- **Efficienza normativa e semplificazione**

Non pertinente.

- **Diritti fondamentali**

La proposta non ha conseguenze prevedibili per la tutela dei diritti fondamentali.

4. INCIDENZA SUL BILANCIO

Nessuna.

5. ALTRI ELEMENTI

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

Le disposizioni che la proposta intende modificare saranno esaminate nell'ambito della valutazione periodica del regolamento sulla cibersicurezza che deve essere svolta dalla Commissione conformemente all'articolo 67 dello stesso. Tale valutazione esamina, tra l'altro, l'impatto, l'efficacia e l'efficienza delle disposizioni del quadro di certificazione della cibersicurezza per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC nell'Unione e di migliorare il funzionamento del mercato interno. La proposta contiene una modifica atta a garantire che la valutazione contempli anche i servizi di sicurezza gestiti. La Commissione invia inoltre una relazione sulla valutazione e le sue conclusioni al Parlamento europeo, al Consiglio e al consiglio di amministrazione dell'ENISA e rende pubblici i risultati della relazione.

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

La proposta comprende due articoli. L'articolo 1 contiene le modifiche del regolamento (UE) 2019/881, mentre l'articolo 2 riguarda l'entrata in vigore. L'articolo 1 contiene modifiche

mirate volte a modificare l'ambito di applicazione del quadro europeo di certificazione della cibersicurezza all'interno del regolamento sulla cibersicurezza, al fine di includere i "servizi di sicurezza gestiti" (articoli 1 e 46 del regolamento sulla cibersicurezza). Introduce una definizione di tali servizi, strettamente allineata alla definizione di "fornitori di servizi di sicurezza gestiti" di cui alla direttiva NIS 2 (articolo 2 del regolamento sulla cibersicurezza). Aggiunge inoltre un nuovo articolo, l'articolo 51 bis, relativo agli obiettivi di sicurezza della certificazione europea della cibersicurezza adeguati ai "servizi di sicurezza gestiti". Infine la proposta contiene varie modifiche tecniche per garantire che i pertinenti articoli si applichino anche ai "servizi di sicurezza gestiti".

2023/0108 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

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

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo,

visto il parere del Comitato delle regioni,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[7] istituisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione.

(2) I servizi di sicurezza gestiti, che consistono nello svolgimento di attività legate alla gestione dei rischi in materia di cibersicurezza dei loro clienti o nella fornitura di assistenza per tali attività, hanno acquisito un'importanza crescente nella prevenzione e attenuazione degli incidenti di cibersicurezza. Di conseguenza i fornitori di tali servizi sono considerati soggetti essenziali o importanti appartenenti a un settore ad alta criticità ai sensi della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[8]. Conformemente al considerando 86 di tale direttiva, i fornitori di servizi di sicurezza gestiti in settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza svolgono un ruolo particolarmente importante nell'assistere i soggetti nei loro sforzi per la prevenzione e il rilevamento degli incidenti, la risposta agli stessi o la ripresa da essi. I fornitori di servizi di sicurezza

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

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

gestiti sono stati tuttavia essi stessi bersaglio di attacchi informatici e presentano un particolare rischio a causa della loro stretta integrazione nelle attività dei clienti. I soggetti essenziali e importanti ai sensi della direttiva (UE) 2022/2555 dovrebbero pertanto esercitare una maggiore diligenza nella selezione di un fornitore di servizi di sicurezza gestiti.

(3) I fornitori di servizi di sicurezza gestiti svolgono inoltre un ruolo importante nel contesto della riserva dell'UE per la cibersicurezza, la cui graduale costituzione è sostenuta dal regolamento (UE) …/…. [che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi]. La riserva dell'UE per la cibersicurezza deve essere utilizzata per sostenere azioni di risposta e di ripresa immediata in caso di incidenti di cibersicurezza gravi e su vasta scala. Il regolamento (UE) …/… [che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi] stabilisce un processo di selezione per i fornitori che costituiscono la riserva dell'UE per la cibersicurezza che dovrebbe, nel cui ambito dovrebbe tra l'altro essere tenuta on considerazione l'eventualità che il fornitore interessato abbia ottenuto una certificazione della cibersicurezza europea o nazionale. I pertinenti servizi erogati da "fornitori di fiducia" conformemente al regolamento (UE) …./… [che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi] corrispondono ai "servizi di sicurezza gestiti" in conformità al presente regolamento.

(4) Oltre a essere rilevante nell'ambito del processo di selezione riguardante la riserva dell'UE per la cibersicurezza, la certificazione dei servizi di sicurezza gestiti rappresenta anche un indicatore di qualità essenziale per i soggetti pubblici e privati che intendono acquistare tali servizi. Alla luce della criticità dei servizi di sicurezza gestiti e della sensibilità dei dati trattati, la certificazione potrebbe fornire ai potenziali clienti indicazioni e garanzie importanti sull'affidabilità di tali servizi. I sistemi europei di certificazione per i servizi di sicurezza gestiti contribuiscono a evitare la frammentazione del mercato unico. Il presente regolamento mira pertanto a migliorare il funzionamento del mercato interno.

(5) Oltre a garantire l'avviamento di prodotti TIC, servizi TIC o processi TIC, i servizi di sicurezza gestiti spesso forniscono funzionalità di servizio aggiuntive basate sulla competenza, sulla perizia e sull'esperienza del personale. Al fine di garantire una qualità molto elevata dei servizi di sicurezza gestiti forniti, occorre prevedere, tra gli obiettivi di sicurezza, competenze, perizia ed esperienza di altissimo livello, nonché procedure interne appropriate. Pertanto, al fine di garantire che tutti gli aspetti relativi ai servizi di sicurezza gestiti siano coperti da un sistema di certificazione, è necessario modificare il regolamento (UE) 2019/881.

Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il [GG/MM/AAAA],

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Modifiche del regolamento (UE) 2019/881

Il regolamento (UE) 2019/881 è così modificato:

1) all'articolo 1, paragrafo 1, primo comma, la lettera b) è sostituita dalla seguente:

"b) un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione.";

2) l'articolo 2 è così modificato:

a) i punti 9, 10 e 11 sono sostituiti dai seguenti:

"9) "sistema europeo di certificazione della cibersicurezza": una serie completa di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti;

10) "sistema nazionale di certificazione della cibersicurezza": una serie completa di regole, requisiti tecnici, norme e procedure elaborati e adottati da un'autorità pubblica nazionale e che si applicano alla certificazione o alla valutazione della conformità dei prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti che rientrano nell'ambito di applicazione del sistema specifico;

11) "certificato europeo di cibersicurezza": un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito è stato oggetto di una valutazione di conformità ai requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;";

b) è inserito il seguente punto:

"14 bis) "servizio di sicurezza gestito": un servizio consistente nello svolgimento di attività legate alla gestione dei rischi in materia di cibersicurezza, tra cui servizi di risposta agli incidenti, test di penetrazione, audit di sicurezza e consulenza, o nella fornitura di assistenza per tali attività";

c) i punti 20, 21 e 22 sono sostituiti dai seguenti:

"20) "specifiche tecniche": un documento che prescrive i requisiti tecnici che un prodotto TIC, un servizio TIC, un processo TIC o un *servizio di sicurezza gestito* deve soddisfare o le relative procedure di valutazione della conformità;

21) "livello di affidabilità": una base per la fiducia nel fatto che un prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito soddisfa i requisiti di sicurezza di uno specifico sistema europeo di certificazione della cibersicurezza e indica il livello al quale un prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito è stato valutato, ma di per sé non misura la sicurezza del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito interessato;

22) "autovalutazione di conformità": un'azione effettuata da un fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza

gestiti, che valuta se tali prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti soddisfino i requisiti di uno specifico sistema europeo di certificazione della cibersicurezza;";

3) all'articolo 4, il paragrafo 6 è sostituito dal seguente:

"6. L'ENISA promuove l'uso della certificazione europea della cibersicurezza, con l'obiettivo di evitare la frammentazione del mercato interno. L'ENISA contribuisce all'istituzione e al mantenimento di un apposito quadro europeo di certificazione della cibersicurezza, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti in termini di cibersicurezza, rafforzando in tal modo la fiducia nel mercato unico digitale e la sua competitività.";

4) l'articolo 8 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

"1. L'ENISA sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti, come stabilito al titolo III del presente regolamento:

a) monitorando continuamente gli sviluppi nei settori di normazione connessi e raccomandando adeguate specifiche tecniche ai fini dello sviluppo di sistemi europei di certificazione della cibersicurezza secondo l'articolo 54, paragrafo 1, lettera c), in assenza di norme;

b) preparando proposte di sistemi europei di certificazione della cibersicurezza ("proposte di sistemi") per prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti conformemente all'articolo 49;

c) valutando i sistemi europei di certificazione della cibersicurezza adottati, conformemente all'articolo 49, paragrafo 8;

d) partecipando a valutazioni inter pares a norma dell'articolo 59, paragrafo 4;

e) assistendo la Commissione nel provvedere alle funzioni di segretariato dell'ECCG a norma dell'articolo 62, paragrafo 5.";

b) il paragrafo 3 è sostituito dal seguente:

"3. L'ENISA elabora e pubblica orientamenti e sviluppa buone pratiche in merito ai requisiti di cibersicurezza per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti, in cooperazione con le autorità nazionali di certificazione della cibersicurezza e con il settore, in modo formale, strutturato e trasparente.";

c) il paragrafo 5 è sostituito dal seguente:

"5. L'ENISA facilita la definizione e l'adozione di norme europee e internazionali in materia di gestione dei rischi e di sicurezza dei prodotti TIC, dei servizi TIC, dei processi TIC e dei servizi di sicurezza gestiti.";

5) all'articolo 46, i paragrafi 1 e 2 sono sostituiti dai seguenti:

"1. È istituito il quadro europeo di certificazione della cibersicurezza al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di cibersicurezza all'interno dell'Unione e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti.

2. Il quadro europeo di certificazione della cibersicurezza prevede un meccanismo volto a istituire sistemi europei di certificazione della cibersicurezza. Tale quadro attesta che i prodotti TIC, servizi TIC e processi TIC valutati nell'ambito di tali sistemi sono conformi a determinati requisiti di sicurezza ai fini della protezione della disponibilità, dell'autenticità, dell'integrità o della riservatezza dei dati conservati, trasmessi o trattati o delle funzioni o dei servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita. Attesta inoltre che i servizi di sicurezza gestiti valutati nell'ambito di tali sistemi sono conformi a determinati requisiti di sicurezza ai fini della protezione della disponibilità, dell'autenticità, dell'integrità e della riservatezza dei dati consultati, trattati, conservati o trasmessi in relazione alla prestazione di tali servizi, e che tali servizi sono forniti continuamente con la competenza, la perizia e l'esperienza richieste da personale avente un elevato livello di conoscenze tecniche pertinenti e integrità professionale.";

6) all'articolo 47, i paragrafi 2 e 3 sono sostituiti dai seguenti:

"2. Il programma di lavoro progressivo dell'Unione include in particolare un elenco di prodotti TIC, servizi TIC e processi TIC, o delle relative categorie, e di servizi di sicurezza gestiti che possono beneficiare dell'inclusione nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza.

3. L'inclusione, nel programma di lavoro progressivo dell'Unione, di specifici prodotti TIC, servizi TIC, processi TIC, o delle relative categorie, o di servizi di sicurezza gestiti è giustificata sulla base di una o più delle seguenti motivazioni:

a) la disponibilità e lo sviluppo di sistemi nazionali di certificazione della cibersicurezza relativi a specifiche categorie di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti e in particolare in relazione al rischio di frammentazione;

b) la pertinente politica o il pertinente diritto dell'Unione o degli Stati membri;

c) la domanda di mercato;

d) gli sviluppi nel panorama delle minacce informatiche;

e) la richiesta di preparazione di una specifica proposta di sistema da parte dell'ECCG.";

7) all'articolo 49, il paragrafo 7 è sostituito dal seguente:

"7. La Commissione, sulla base della proposta di sistema preparata dall'ENISA, può adottare atti di esecuzione, prevedendo un sistema europeo di

certificazione della cibersicurezza per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti che soddisfano i requisiti di cui agli articoli 51, 52 e 54. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 66, paragrafo 2.";

8) l'articolo 51 è così modificato:

a) il titolo è sostituito dal seguente:

Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza per prodotti TIC, servizi TIC e processi TIC

b) la frase introduttiva è sostituita dalla seguente:

"I sistemi europei di certificazione della cibersicurezza per i prodotti TIC, i servizi TIC o i processi TIC sono progettati per conseguire, se del caso, almeno i seguenti obiettivi di sicurezza:";

9) è inserito l'articolo seguente:

"Articolo 51 bis

Obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti

"I sistemi europei di certificazione della cibersicurezza per i servizi di sicurezza gestiti sono progettati per conseguire, se del caso, almeno i seguenti obiettivi di sicurezza:

a) garantire che i servizi di sicurezza gestiti siano forniti con la competenza, la perizia e l'esperienza richieste e che il personale responsabile della prestazione di tali servizi possieda un elevato livello di conoscenze e competenze tecniche nel settore specifico, un'esperienza sufficiente e appropriata e la massima integrità professionale;

b) garantire che il fornitore predisponga procedure interne appropriate affinché i servizi di sicurezza gestiti forniti abbiano sempre un livello di qualità molto elevato;

c) proteggere i dati consultati, conservati, trasmessi o altrimenti trattati in relazione alla fornitura dei servizi di sicurezza gestiti dall'accesso, dall'archiviazione, dalla divulgazione, dalla distruzione, da altro trattamento, dalla perdita o dall'alterazione accidentali o non autorizzati oppure dalla mancanza di disponibilità;

d) garantire che la disponibilità e l'accesso ai dati, ai servizi e alle funzioni siano ripristinati in modo tempestivo in caso di incidente fisico o tecnico;

e) garantire che le persone, i programmi o le macchine autorizzati possano accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso;

f) registrare e permettere di valutare a quali dati, servizi o funzioni è stato effettuato l'accesso e quali sono stati utilizzati o altrimenti trattati, in quale momento e da chi;

g) garantire che i prodotti TIC, i servizi TIC e i processi TIC [e l'hardware] avviati nella fornitura dei servizi di sicurezza gestiti siano sicuri fin dalla progettazione e per impostazione predefinita, non contengano vulnerabilità note e includano gli ultimi aggiornamenti connessi alla sicurezza;";

10) l'articolo 52 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

"1. I sistemi europei di certificazione della cibersicurezza possono specificare per i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti uno o più dei seguenti livelli di affidabilità: "di base", "sostanziale" o "elevato". Il livello di affidabilità è commisurato al livello del rischio associato al previsto uso del prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito, in termini di probabilità e impatto di un incidente.";

b) il paragrafo 3 è sostituito dal seguente:

"3. I requisiti di sicurezza corrispondenti a ogni livello di affidabilità sono indicati nel sistema europeo di certificazione della cibersicurezza pertinente, comprese le corrispondenti funzionalità di sicurezza e il rigore e la specificità corrispondenti della valutazione a cui deve essere sottoposto il prodotto TIC, servizio TIC, processo TIC o servizio di sicurezza gestito.";

c) i paragrafi 5, 6 e 7 sono sostituiti dai seguenti:

"5. Un certificato europeo di cibersicurezza o una dichiarazione UE di conformità che si riferisca al livello di affidabilità "di base" assicura che i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti per i quali sono rilasciati tale certificato o tale dichiarazione UE di conformità rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi di base noti di incidenti e attacchi informatici. Le attività di valutazione da intraprendere comprendono almeno un riesame della documentazione tecnica. Qualora tale riesame non sia appropriato, si ricorre ad attività di valutazione sostitutive di effetto equivalente.

6. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità "sostanziale" assicura che i prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo i rischi noti connessi alla cibersicurezza e i rischi di incidenti e di attacchi informatici causati da soggetti dotati di abilità e risorse limitate. Le attività di valutazione da intraprendere comprendono almeno: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti attuano correttamente

le necessarie funzionalità di sicurezza. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività di valutazione sostitutive di effetto equivalente.

7. Un certificato europeo di cibersicurezza che si riferisca al livello di affidabilità "elevato" assicura che i prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti per i quali è rilasciato tale certificato rispettano i corrispondenti requisiti di sicurezza, comprese le funzionalità di sicurezza, e sono stati valutati a un livello inteso a ridurre al minimo il rischio di attacchi informatici avanzati commessi da attori che dispongono di abilità e risorse significative. Le attività di valutazione da intraprendere comprendono almeno: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti attuano correttamente le necessarie funzionalità di sicurezza, allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione. Qualora tali attività di valutazione non siano appropriate, si ricorre ad attività sostitutive di effetto equivalente.";

11) all'articolo 53, i paragrafi 1, 2 e 3 sono sostituiti dai seguenti:

"1. Un sistema europeo di certificazione della cibersicurezza può consentire un'autovalutazione della conformità sotto la sola responsabilità del fabbricante o del fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti. Tale autovalutazione della conformità è consentita unicamente in relazione ai prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti che presentano un basso rischio corrispondente al livello di affidabilità "di base".

2. Il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o di servizi di sicurezza gestiti può rilasciare una dichiarazione UE di conformità in cui afferma che è stato dimostrato il rispetto dei requisiti previsti nel sistema. Rilasciando tale dichiarazione, il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti si assume la responsabilità della conformità del prodotto TIC, servizio TIC, processo TIC o del servizio di sicurezza gestito ai requisiti previsti in tale sistema.

3. Il fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti rende disponibile all'autorità nazionale di certificazione della cibersicurezza di cui all'articolo 58, per il periodo stabilito nel corrispondente sistema europeo di certificazione della cibersicurezza, la dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti relative alla conformità al sistema dei prodotti TIC, servizi TIC o servizi di sicurezza gestiti. Una copia della dichiarazione UE di conformità è trasmessa all'autorità nazionale di certificazione della cibersicurezza e all'ENISA.";

12) all'articolo 54, il paragrafo 1 è così modificato:

a) la lettera a) è sostituita dalla seguente:

"a) l'oggetto e l'ambito di applicazione del sistema di certificazione, compresi il tipo o le categorie di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti coperti;";

b) la lettera j) è sostituita dalla seguente:

"j) le regole per il controllo della conformità dei prodotti TIC, servizi TIC, processi TIC e dei servizi di sicurezza gestiti ai requisiti dei certificati europei di cibersicurezza o delle dichiarazioni UE di conformità, compresi i meccanismi per dimostrare il mantenimento della conformità ai requisiti di cibersicurezza specificati;";

c) la lettera l) è sostituita dalla seguente:

"l) le regole riguardanti le conseguenze per i prodotti TIC, servizi TIC, processi TIC e i servizi di sicurezza gestiti che sono stati certificati o per i quali è stata rilasciata una dichiarazione UE di conformità ma che non sono conformi ai requisiti del sistema;";

d) la lettera o) è sostituita dalla seguente:

"o) l'individuazione dei sistemi nazionali o internazionali di certificazione della cibersicurezza relativi allo stesso tipo o alle stesse categorie di prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti, requisiti di sicurezza, criteri e metodi di valutazione nonché livelli di affidabilità;";

e) la lettera q) è sostituita dalla seguente:

"q) il periodo di disponibilità della dichiarazione UE di conformità, la documentazione tecnica e tutte le altre informazioni pertinenti che devono essere rese disponibili dal fabbricante o fornitore di prodotti TIC, servizi TIC, processi TIC o di servizi di sicurezza gestiti;";

13) l'articolo 56 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

"1. I prodotti TIC, i servizi TIC, i processi TIC e i servizi di sicurezza gestiti certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 sono considerati conformi ai requisiti di tale sistema.";

b) il paragrafo 3 è così modificato:

i) il primo comma è sostituito dal seguente:

"La Commissione valuta periodicamente l'efficacia e l'utilizzo dei sistemi europei di certificazione della cibersicurezza adottati e l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersicurezza per mezzo di disposizioni normative dell'Unione pertinenti al fine di garantire l'opportuno livello di cibersicurezza dei prodotti TIC, servizi TIC, processi TIC e dei servizi di sicurezza gestiti nell'Unione e migliorare il funzionamento

del mercato interno. La prima valutazione di questo genere è effettuata entro il 31 dicembre 2023 e le successive valutazioni sono effettuate almeno ogni due anni. Sulla base dei risultati di tali valutazioni, la Commissione individua i prodotti TIC, servizi TIC, processi TIC e i servizi di sicurezza gestiti coperti da un sistema di certificazione esistente che devono rientrare in un sistema obbligatorio di certificazione.";

ii) il terzo comma è così modificato:

aa) la lettera a) è sostituita dalla seguente:

"a) prende in considerazione l'impatto delle misure sui fabbricanti o fornitori di tali prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti e sugli utenti in termini di costi di tali misure nonché i benefici sociali o economici derivanti dal previsto aumento del livello di sicurezza per i prodotti TIC, i servizi TIC, i processi TIC o i servizi di sicurezza gestiti in questione;";

bb) la lettera d) è sostituita dalla seguente:

"d) prende in considerazione le scadenze di attuazione e le misure transitorie e i periodi di transizione, in particolare con riferimento al possibile impatto delle misure sui fornitori o fabbricanti di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti, PMI comprese;";

c) i paragrafi 7 e 8 sono sostituiti dai seguenti:

"7. La persona fisica o giuridica che presenta i prodotti TIC, servizi TIC, processi TIC o i servizi di sicurezza gestiti per la certificazione mette a disposizione dell'autorità nazionale di certificazione della cibersicurezza di cui all'articolo 58, qualora tale autorità sia l'organismo che rilascia il certificato europeo di cibersicurezza, o dell'organismo di valutazione della conformità di cui all'articolo 60 tutte le informazioni necessarie a espletare la certificazione.

8. Il titolare di un certificato europeo di cibersicurezza informa l'autorità o l'organismo di cui al paragrafo 7 delle eventuali vulnerabilità o irregolarità successivamente rilevate in relazione alla sicurezza dei prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti certificati che possono incidere sulla conformità ai requisiti relativi alla certificazione. Tale autorità o organismo trasmette tali informazioni senza indebiti ritardi all'autorità nazionale di certificazione della cibersicurezza interessata.";

14) all'articolo 57, i paragrafi 1 e 2 sono sostituiti dai seguenti:

"1. Fatto salvo il paragrafo 3 del presente articolo, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 49, paragrafo 7. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti TIC, servizi TIC, processi TIC e per i servizi di sicurezza gestiti non coperti da un sistema europeo di certificazione della cibersicurezza restano in vigore.

2. Gli Stati membri non introducono nuovi sistemi nazionali di certificazione della cibersicurezza per prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti già coperti da un sistema europeo di certificazione della cibersicurezza in vigore.";

15) l'articolo 58 è così modificato:

a) il paragrafo 7 è così modificato:

i) le lettere a) e b) sono sostituite dalle seguenti:

"a) supervisionano e fanno applicare le regole previste nei sistemi europei di certificazione della cibersicurezza a norma dell'articolo 54, paragrafo 1, lettera j), per il controllo della conformità dei prodotti TIC, servizi TIC, processi TIC e dei servizi di sicurezza gestiti ai requisiti dei certificati europei di cibersicurezza rilasciati nei rispettivi territori, in cooperazione con altre autorità di vigilanza del mercato competenti;

b) controllano la conformità agli obblighi e fanno applicare gli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC, processi TIC o servizi di sicurezza gestiti che sono stabiliti nei rispettivi territori e che effettuano un'autovalutazione della conformità, e in particolare controllano la conformità agli obblighi e fanno applicare gli obblighi incombenti a tali fabbricanti o fornitori di cui all'articolo 53, paragrafi 2 e 3, e nel corrispondente sistema europeo di certificazione della cibersicurezza;";

ii) la lettera h) è sostituita dalla seguente:

"h) cooperano con le altre autorità nazionali di certificazione della cibersicurezza o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali prodotti TIC, servizi TIC, processi TIC e servizi di sicurezza gestiti non conformi ai requisiti del presente regolamento o ai requisiti di specifici sistemi europei di certificazione della cibersicurezza; e";

b) il paragrafo 9 è sostituito dal seguente:

"9. Le autorità nazionali di certificazione della cibersicurezza cooperano tra di loro e con la Commissione, in particolare scambiandosi informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le questioni tecniche riguardanti la cibersicurezza di prodotti TIC, servizi TIC, processi TIC e di servizi di sicurezza gestiti.";

16) all'articolo 59, paragrafo 3, le lettere b) e c) sono sostituite dalle seguenti:

"b) le procedure di supervisione e applicazione delle regole per il controllo della conformità dei prodotti TIC, servizi TIC, processi TIC e dei servizi di sicurezza gestiti con i certificati europei di cibersicurezza a norma dell'articolo 58, paragrafo 7, lettera a);

c) le procedure di monitoraggio e applicazione degli obblighi che incombono ai fabbricanti o ai fornitori di prodotti TIC, servizi TIC, processi TIC o di servizi di sicurezza gestiti a norma dell'articolo 58, paragrafo 7, lettera b);";

17) all'articolo 67, i paragrafi 2 e 3 sono sostituiti dai seguenti:

"2. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III del presente regolamento per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti TIC, servizi TIC, processi TIC e dei servizi di sicurezza gestiti nell'Unione e di migliorare il funzionamento del mercato interno.

3. La valutazione esamina se siano necessari requisiti essenziali di cibersicurezza per l'accesso al mercato interno onde impedire l'ingresso nel mercato dell'Unione di prodotti TIC, servizi TIC, processi TIC e di servizi di sicurezza gestiti che non rispettano i requisiti di base in materia di cibersicurezza.".

Articolo 2

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

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

Fatto a Strasburgo, il

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