Parlamento europeo
2019-2024

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

2023/0108(COD)

7.9.2023

***I
PROGETTO DI RELAZIONE

sulla proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

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

Relatrice: Josianne Cutajar

Significato dei simboli utilizzati

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

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

Emendamenti a un progetto di atto

Emendamenti del Parlamento presentati su due colonne

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

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

Emendamenti del Parlamento presentati in forma di testo consolidato

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

INDICE

Pagina

PROGETTO DI RISOLUZIONE LEGISLATIVA DEL PARLAMENTO EUROPEO 5

MOTIVAZIONE.....15

ALLEGATO: ELENCO DELLE ENTITÀ O DELLE PERSONE DA CUI IL RELATORE PER PARERE HA RICEVUTO CONTRIBUTI.....16

PROGETTO DI RISOLUZIONE LEGISLATIVA DEL PARLAMENTO EUROPEO

sulla proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

(Procedura legislativa ordinaria: prima lettura)

Il Parlamento europeo,

– vista la proposta della Commissione al Parlamento europeo e al Consiglio (COM(2023)0208),

– visti l'articolo 294, paragrafo 2, e l'articolo 114 del trattato sul funzionamento dell'Unione europea, a norma dei quali la proposta gli è stata presentata dalla Commissione (C9-0137/2023),

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

– visto il parere del Comitato economico e sociale europeo del 13 luglio 2023[1],

– visto l'articolo 59 del suo regolamento,

– vista la lettera della commissione per il mercato interno e la protezione dei consumatori,

– vista la relazione della commissione per l'industria, la ricerca e l'energia (A9-0000/2023),

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

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

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

[1] GU C 0 del 0.0.0000, pag. 0. / Non ancora pubblicato nella Gazzetta ufficiale.

Emendamento 1

Proposta di regolamento
Considerando 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	(1 bis) Al fine di garantire la resilienza dell'Unione agli attacchi informatici e prevenire eventuali vulnerabilità nel mercato dell'Unione, il presente regolamento integrerà il quadro normativo orizzontale che stabilisce requisiti globali di cibersicurezza per tutti i prodotti con elementi digitali conformemente al regolamento (UE) .../... del Parlamento europeo e del Consiglio*[*] [+], definendo requisiti essenziali per i servizi di cibersicurezza gestiti, la loro applicazione e la loro affidabilità.

[*] Regolamento (UE) .../... del Parlamento europeo e del Consiglio, del ..., ...

(GU ...).

[+] GU: inserire nel testo il numero del regolamento contenuto nel documento 2022/0272(COD) e inserire, nella nota a piè di pagina, il numero, la data, il titolo e il riferimento alla Gazzetta ufficiale del regolamento.

Or. en

Emendamento 2

Proposta di regolamento
Considerando 2

Testo della Commissione	*Emendamento*
(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	(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, ***incluse la prevenzione e il rilevamento degli incidenti, la risposta agli stessi o la***

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 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.

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 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.

[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)

[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).

(GU L 333 del 27.12.2022, pag. 80).

Or. en

Emendamento 3

Proposta di regolamento
Considerando 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	(4 bis) I sistemi europei di certificazione per i servizi di sicurezza gestiti dovrebbero contribuire all'accessibilità, anche economica, di tali servizi, in particolare per gli attori di dimensioni più ridotte, come le microimprese e le piccole e medie imprese, che sono esposti più di frequente a violazioni della cibersicurezza con implicazioni finanziarie, giuridiche, reputazionali e operative.

Or. en

Emendamento 4

Proposta di regolamento
Considerando 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	(5 bis) Al fine di agevolare la crescita di un mercato dell'Unione affidabile, creando nel contempo partenariati con paesi terzi affini, anche alla luce delle disposizioni del regolamento (UE) .../... del Parlamento europeo e del Consiglio [*] ***[++] relativamente all'accesso alla riserva dell'UE per la cibersicurezza, il processo di certificazione stabilito nel quadro istituito dal presente regolamento dovrebbe essere razionalizzato per garantire il riconoscimento internazionale e l'allineamento alle norme internazionali.***

[*] Regolamento (UE) .../... del Parlamento

europeo e del Consiglio, del ..., ...

(GU ...).

++ GU: inserire nel testo il numero del regolamento contenuto nel documento 2023/0109(COD) e inserire, nella nota a piè di pagina, il numero, la data, il titolo e il riferimento alla Gazzetta ufficiale del regolamento.

Or. en

Emendamento 5

Proposta di regolamento
Considerando 5 ter (nuovo)

Testo della Commissione	*Emendamento*
	(5 ter) Allo scopo di garantire lo sviluppo di un mercato dell'Unione affidabile per i servizi di sicurezza gestiti, i relativi fornitori e gli Stati membri dovrebbero collaborare e contribuire alla raccolta su vasta scala di dati sullo stato e sull'evoluzione del mercato del lavoro della cibersicurezza.

Or. en

Emendamento 6

Proposta di regolamento
Considerando 5 quater (nuovo)

Testo della Commissione	*Emendamento*
	(5 quater) Un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche si basa sullo sviluppo delle capacità degli Stati membri. Come riconosciuto nella recente comunicazione della Commissione dell'8 aprile 2023 dal titolo "Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE", la sicurezza dell'UE non può essere garantita senza il bene più prezioso dell'UE: la sua popolazione. Pertanto,

qualsiasi sistema europeo di certificazione dovrebbe prendere in considerazione l'assistenza agli Stati membri, anche per quanto riguarda il divario di competenze in materia di cibersicurezza.

Or. en

Emendamento 7

Proposta di regolamento
Considerando 5 quinquies (nuovo)

Testo della Commissione	*Emendamento*
	(5 quinquies) Alla luce dell'elaborazione e dell'attuazione del sistema europeo di certificazione per i servizi di sicurezza gestiti, la Commissione dovrebbe intensificare gli scambi con l'ENISA e agevolare il dialogo con gli Stati membri, il settore privato e il mondo accademico, al fine di comprendere meglio la composizione della forza lavoro dell'Unione nel settore della cibersicurezza e delle competenze associate.

Or. en

Emendamento 8

Proposta di regolamento
Considerando 5 sexies (nuovo)

Testo della Commissione	*Emendamento*
	(5 sexies) Al fine di consentire ai sistemi europei di cibersicurezza di attestare che i servizi di sicurezza gestiti valutati nell'ambito di tali sistemi sono conformi a determinati requisiti di sicurezza, anche in relazione alla continua fornitura di tali servizi con la competenza, la perizia e l'esperienza richieste a opera di personale avente un elevato livello di conoscenze tecniche pertinenti e integrità professionale in conformità al presente regolamento, i

sistemi dovrebbero ricorrere al contributo del mondo accademico, degli istituti di ricerca e di altri portatori di interessi con esperienza nella formazione di professionisti della cibersicurezza, nell'attrarre, assumere e sviluppare talenti, nonché nell'incentivare partenariati pubblico-privati. Dovrebbe fungere da catalizzatore per la messa in comune di idee e la condivisione di competenze in materia di formazione e per una migliore valutazione delle competenze necessarie, in particolare durante il processo di assunzione. Oltre a contribuire al sistema, il settore privato dovrebbe anche mirare a fornire una formazione sul posto di lavoro che affronti le competenze più richieste, coinvolgendo l'amministrazione pubblica e le start-up, nonché le microimprese e le piccole e medie imprese.

Or. en

Emendamento 9

Proposta di regolamento
Considerando 5 septies (nuovo)

Testo della Commissione	*Emendamento*
	(5 septies) Al fine di facilitare l'emergere di servizi di sicurezza gestiti essenziali e di elevata qualità, gli Stati membri dovrebbero adottare attivamente misure per formare e trattenere i talenti, in particolare integrando la cibersicurezza nei programmi di istruzione e formazione, garantendo al contempo l'accesso agli apprendistati e ai tirocini per i giovani, specialmente le persone che vivono in regioni svantaggiate, come le isole e le regioni scarsamente popolate, rurali e periferiche. Tali misure dovrebbero altresì mirare ad attirare un maggior numero di donne e di ragazze nel settore e contribuire ad affrontare il divario di genere nel campo della scienza, della tecnologia, dell'ingegneria e della

matematica.

Or. en

Emendamento 10

Proposta di regolamento
Articolo 1 – punto 2 – lettera b
Regolamento (UE) 2019/881
Articolo 2 – punto 14 bis

Testo della Commissione	*Emendamento*
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";	14 bis) "servizio di sicurezza gestito": un servizio ***esternalizzato*** consistente nello svolgimento di attività legate alla gestione dei rischi in materia di cibersicurezza, tra cui servizi di ***prevenzione e rilevamento degli incidenti,*** risposta agli stessi ***o ripresa da essi***, test di penetrazione, audit di sicurezza e consulenza, o nella fornitura di assistenza per tali attività";

Or. en

Emendamento 11

Proposta di regolamento
Articolo 1 – punto 6
Regolamento (UE) 2019/881
Articolo 47 – paragrafo 3 – lettera e bis (nuovo)

Testo della Commissione	*Emendamento*
	e bis) l'allineamento preventivo alle norme internazionali applicabili;

Or. en

Emendamento 12

Proposta di regolamento
Articolo 1 – punto 6
Regolamento (UE) 2019/881
Articolo 47 – paragrafo 3 – lettera e ter (nuovo)

Testo della Commissione	*Emendamento*
	e ter) il contributo del fornitore di servizi di sicurezza gestiti all'offerta di opportunità di formazione e di miglioramento del livello delle competenze al personale allo scopo di conseguire un elevato livello di conoscenze tecniche pertinenti e integrità professionale.

Or. en

Emendamento 13

Proposta di regolamento
Articolo 1 – punto 6
Regolamento (UE) 2019/881
Articolo 47 – paragrafo 3 bis (nuovo)

Testo della Commissione	*Emendamento*
	3 bis. Inoltre, l'inclusione di servizi di sicurezza gestiti specifici nel programma di lavoro progressivo dell'Unione tiene conto, se del caso, del contributo dei fornitori di servizi di sicurezza gestiti alla formazione e all'attrazione di talenti, specialmente attraverso partenariati con università e altri istituti di istruzione.

Or. en

Emendamento 14

Proposta di regolamento
Articolo 1 – punto 7
Regolamento (UE) 2019/881
Articolo 49 – paragrafo 7 bis (nuovo)

Testo della Commissione	*Emendamento*
	7 bis. La proposta di sistema è elaborata tenendo conto di ogni contributo fornito dal sistema europeo di normazione tecnica o dalle agenzie settoriali dell'Unione.

Or. en

Emendamento 15

Proposta di regolamento
Articolo 1 – punto 9
Regolamento (UE) 2019/881
Articolo 51 bis – lettera b

Testo della Commissione	*Emendamento*
b) garantire che il fornitore predisponga procedure interne appropriate affinché i servizi di sicurezza gestiti forniti abbiano sempre un livello di qualità molto elevato;	b) garantire che il fornitore predisponga procedure interne appropriate affinché i servizi di sicurezza gestiti forniti abbiano sempre un livello di qualità ***e di affidabilità*** molto elevato;

Or. en

Emendamento 16

Proposta di regolamento
Articolo 1 – punto 13 – lettera b – punto ii – lettera bb
Regolamento (UE) 2019/881
Articolo 56 – paragrafo 3 – lettera d

Testo della Commissione	*Emendamento*
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;***";	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, ***inclusi gli interessi e i fabbisogni specifici delle microimprese e delle piccole e medie imprese. La Commissione garantisce un adeguato sostegno finanziario nel quadro normativo dei programmi dell'Unione esistenti, in particolare al fine di alleggerire l'onere finanziario per le microimprese e le piccole e medie imprese***;";

Or. en

MOTIVAZIONE

La relatrice appoggia la proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti considerando la necessità di aggiornare e rafforzare il sistema europeo di certificazione della cibersicurezza di modo che copra servizi industriali importanti e in crescita. Visto che alcuni Stati membri hanno già iniziato ad adottare sistemi di certificazione per i servizi di sicurezza gestiti, la relatrice è del parere che questa modifica del regolamento dell'UE sulla cibersicurezza sia fondamentale per evitare importanti divergenze tra i sistemi nazionali, che comporterebbero una forma di frammentazione del mercato che è contraria agli interessi economici e strategici dell'Unione.

A tale riguardo, si prende atto che la proposta in esame è complementare al regolamento sulla cibersolidarietà e che questa specifica estensione al sistema europeo di certificazione della cibersicurezza consentirà ai fornitori di servizi di sicurezza gestiti – che corrispondono ai "fornitori di fiducia" nel regolamento sulla cibersolidarietà – di svolgere un ruolo importante nel contesto della futura riserva per la cibersicurezza a livello di UE. Pertanto, la proposta riveste una grande importanza per promuovere una maggiore capacità dell'Unione in materia di cibersicurezza, che è essenziale per contrastare potenziali minacce in una realtà geopolitica in costante evoluzione.

Entro i limiti della proposta della Commissione, l'obiettivo della relatrice è di consolidare questa modifica mirata del regolamento sulla cibersicurezza e di renderla più chiara. Ciò è illustrato dall'emendamento presentato dalla relatrice per quanto riguarda la definizione di servizi di sicurezza gestiti, che precisa che tali servizi sono "esternalizzati" e specifica meglio cosa include la definizione. Gli emendamenti presentati riguardanti il riconoscimento delle norme internazionali in materia di cibersicurezza sono intesi a promuovere un più elevato livello di fiducia definendo al contempo norme globali a livello di UE.

Il presente progetto di relazione mette in maggiore rilievo la necessità di affrontare il divario di competenze in materia di cibersicurezza e di sostenere le microimprese e le piccole e medie imprese. Per quanto riguarda il primo aspetto, gli emendamenti presentati si basano sulla necessità già implicita di competenze nel quadro del sistema di certificazione della cibersicurezza per quanto riguarda "la competenza, la perizia e l'esperienza richieste da personale avente un elevato livello di conoscenze tecniche pertinenti e integrità professionale". Secondo la relatrice, il sistema europeo di certificazione non deve solo promuovere la cooperazione tra tutti gli attori interessati come pure tra gli Stati membri, il settore privato, il mondo accademico e gli istituti di ricerca, ma deve anche incoraggiare la definizione di una nuova tabella di marcia per formare e rendere autonoma la forza lavoro, raccogliendo un maggior numero di dati sulle competenze necessarie e contribuendo ad affrontare il divario di genere nel campo della scienza, della tecnologia, dell'ingegneria e della matematica (STEM).

Al tempo stesso, le microimprese e le piccole e medie imprese, che costituiscono la spina dorsale dell'economia europea e hanno sicuramente un ruolo positivo da svolgere nel settore della cibersicurezza, dovrebbero beneficiare di un sostegno finanziario adeguato nel quadro normativo dei programmi dell'Unione esistenti al fine di alleggerire qualsiasi onere finanziario sproporzionato che grava su di esse.

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 della relatrice. La relatrice ha ricevuto contributi dalle seguenti entità o persone per la preparazione del progetto di relazione sulla *proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti 2023/0108(COD)*.

Entity and/or person
European Economic and Social Committee
European Commission
ENISA
Leonardo Cyber and Security Solutions
Red Alert Labs IoT Security
ESET Slovak
Board of Cyber
IBM
Tecnalia
FERMA - Federation of European Risk Management Associations