Relazione

ai sensi dell'art. 6, comma 4, della legge n. 234/2012

Oggetto dell'atto:
Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti
– **Codice della proposta:** COM (202) 208 del 21/04/2023
– **Codice interistituzionale:** 2023/0108(COD)
– **Amministrazione con competenza prevalente:** Agenzia per la cybersicurezza nazionale

***

Premessa: finalità e contesto

La proposta di regolamento mira ed emendare il 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 cybersicurezza»), entrato in vigore il 28 giugno 2021.

In particolare, il Titolo III del suddetto Regolamento ha introdotto nell'Unione europea un quadro europeo di certificazione per la cybersicurezza di prodotti TIC (Tecnologie dell'Informazione e delle Comunicazioni), servizi TIC e processi TIC. La finalità della proposta emendativa riguarda l'adozione di sistemi europei di certificazione della cybersicurezza per i «servizi di sicurezza gestiti» oltre che per i prodotti relativi alle tecnologie dell'informazione (TIC), i servizi TIC e i processi TIC, già previsti dal regolamento sulla cybersicurezza.

Al predetto fine, la presente proposta legislativa inserisce nell'articolo 2 del regolamento (UE) 2019/881, il punto 14 bis, recante la definizione di «servizi di sicurezza gestiti», ossia, "un servizio consistente nello svolgimento di attività legate alla gestione dei rischi in materia di cybersicurezza, tra cui servizi di risposta agli incidenti, test di penetrazione, audit di sicurezza e consulenza, o nella fornitura di assistenza per tali attività". Gli obiettivi di sicurezza dei sistemi europei di certificazione della cybersicurezza per i «servizi di sicurezza gestiti» sono definiti nel nuovo articolo 51 bis che indica per tali soggetti che forniscono tali servizi specifici requisiti di competenza e tecnico-organizzativi, con particolare riguardo al trattamento dei dati, all'archiviazione degli stessi e relativo accesso, nonché in merito alle caratteristiche dei prodotti, servizi, processi e hardware forniti nell'ambito dei «servizi di sicurezza gestiti» che dovranno possedere caratteristiche di resilienza, progettazione sicura, assenza di vulnerabilità ed aggiornamento continuo. La proposta introduce alcune ulteriori modifiche formali al regolamento (UE) 2019/881 per estendere l'ambito della certificazione ai «servizi di sicurezza gestiti».

La crescente importanza che hanno acquisito i «servizi di sicurezza gestiti» nella prevenzione e attenuazione degli incidenti di cybersicurezza ha avuto come conseguenza che i fornitori di servizi di sicurezza gestiti siano ritenuti soggetti essenziali o importanti appartenenti a un settore ad alta criticità, ai sensi della direttiva (UE) 2022/2555 (cosiddetta direttiva NIS 2). Nel considerando 86 della direttiva medesima si afferma, infatti, 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 possono essere potenzialmente un fattore di rischio e di vulnerabilità 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 è complementare alla proposta di regolamento sulla cybersolidarietà (COM(2023) 209 del 18/04/2023), che disciplina le modalità di costituzione della "riserva per la cybersicurezza" a livello di UE; tale proposta, infatti, nello stabilire un processo di selezione dei fornitori per la costituzione della riserva considera, tra l'altro, se gli stessi abbiano ottenuto una certificazione della cybersicurezza europea o nazionale. I futuri sistemi di certificazione per i «servizi di sicurezza gestiti» svolgeranno, pertanto, un ruolo significativo nell'attuazione del regolamento sulla cybersolidarietà.

- quadro normativo:

Un invito all'Unione e ai suoi Stati membri a intensificare gli sforzi tesi ad accrescere il livello complessivo della cybersicurezza è stato rivolto dal Consiglio già nelle sue conclusioni del 23 maggio 2022 sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica e, tra le azioni proposte, vi è proprio l'obiettivo di favorire la crescita e lo sviluppo di fornitori di servizi di cybersicurezza gestiti che siano affidabili, sottolineando come lo sviluppo di tali fornitori dovrebbe essere prioritario per la politica industriale dell'Unione nel settore della cybersicurezza. Il Consiglio ha, inoltre, invitato la Commissione a proporre azioni tese a incoraggiare l'emergere di un'industria di servizi di cybersicurezza affidabile.

Inoltre, nella comunicazione congiunta "La politica di ciberdifesa dell'UE" (JOIN(2022) 49 final), adottata dalla Commissione e dall'alto rappresentante il 10 novembre 2022, è stato annunciato che la Commissione vaglierà lo sviluppo di sistemi di certificazione della cybersicurezza a livello UE per l'industria della cybersicurezza e le imprese private, in considerazione, come poc'anzi richiamato, dell'importanza che anche i fornitori di servizi di sicurezza gestiti svolgeranno nel contesto della riserva per la cybersicurezza a livello di UE, la cui costituzione graduale è sostenuta dal richiamato regolamento sulla cybersolidarietà.

A. Rispetto dei principi dell'ordinamento europeo

1. Rispetto del principio di attribuzione, con particolare riguardo alla correttezza della base

giuridica

La proposta rispetta il principio di attribuzione in quanto conforme all'articolo 5.2 del trattato sull'Unione europea (TUE) ai sensi del quale l'Unione europea agisce esclusivamente nei limiti delle competenze che le sono attribuite nei trattati dell'UE.

Le azioni poste in essere con la presente proposta di regolamento, infatti, non vanno oltre quanto necessario per raggiungere i suoi obiettivi generali e specifici e, come evidenziato nella relazione in premessa, ugualmente al regolamento (UE) 2019/881 che mira ad integrare, è volta ad ottenere un'armonizzazione dei servizi del mercato interno dell'Unione europea ai sensi dell'articolo 114 del TFUE.

2. Rispetto del principio di sussidiarietà

La proposta rispetta il principio di sussidiarietà in quanto conforme all'articolo 5.3 del trattato sull'Unione europea (TUE) che esclude l'intervento dell'Unione quando una questione può essere regolata in modo efficace dagli Stati membri stessi a livello centrale, regionale o locale.

Infatti, l'obiettivo di rendere possibile l'adozione di sistemi europei di certificazione della cybersicurezza 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.

3. Rispetto del principio di proporzionalità

La proposta rispetta il principio di proporzionalità in quanto conforme all'articolo 5.4 del trattato sull'Unione europea (TUE) che stabilisce che il contenuto e la forma dell'azione dell'Unione devono limitarsi a quanto necessario per il conseguimento degli obiettivi dei trattati.

Infatti, come evidenziato, la proposta legislativa modifica in maniera specifica il regolamento (UE) 2019/881 limitatamente a quanto strettamente necessario per conseguire il suo obiettivo di rendere possibile l'adozione di sistemi europei di certificazione della cybersicurezza 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 cybersicurezza 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 cybersicurezza 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».

B. Valutazione complessiva del progetto e delle sue prospettive negoziali

1. Valutazione del progetto e urgenza

La valutazione delle finalità generali del progetto è complessivamente positiva in quanto mira ad adottare i sistemi europei di certificazione della cybersicurezza per i «servizi di sicurezza gestiti», già diffusi nell'Unione europea, stabilendo per gli stessi dei requisiti generali di qualità e tecnico-

organizzativi certificabili ai sensi del regolamento (UE) 2019/881, riducendo così la frammentazione introdotta da eventuali norme nazionali ed elevando nel complesso il livello di protezione dalle minacce di cybersicurezza per le imprese operanti nell'Unione europea.

L'integrazione dei «servizi di sicurezza gestiti» nel regolamento (UE) 2019/881 appare urgente anche per rafforzare il nuovo quadro già definito dalla direttiva NIS 2, oltreché la proposta di regolamento sulla cybersolidarietà avanzata dalla Commissione europea in contemporanea con la presente proposta.

Inoltre, poiché i «servizi di sicurezza gestiti», oltre a garantire l'avviamento di prodotti TIC, servizi TIC o processi TIC, spesso forniscono funzionalità di servizio aggiuntive basate sulla competenza, sulla perizia e sull'esperienza del personale, risulta necessario garantire che tutti gli aspetti relativi a tali servizi siano coperti da un sistema di certificazione e, dunque, occorre modificare in tal senso il regolamento (UE) 2019/881. Infatti, un fabbricante di prodotti TIC o fornitore di servizi TIC, con la certificazione di «servizi di sicurezza gestiti», dispone di un ulteriore strumento per incrementare la sicurezza di prodotti TIC o servizi TIC da immettere sul mercato. In particolare, il fabbricante di prodotti TIC o fornitore di servizi TIC, per incrementare la sicurezza dei prodotti TIC, servizi TIC da esso forniti potrà ottenere assistenza da un soggetto certificato per erogare servizi di sicurezza gestiti, con le competenze necessarie, gli strumenti e l'organizzazione idonea per fornire tale assistenza.

Premessa, dunque, una valutazione positiva della proposta legislativa nel suo complesso è, tuttavia, da evidenziare che la possibilità di fare ricorso all'utilizzo di «servizi di sicurezza gestiti» potrebbe nel tempo sostituire le procedure di certificazione di prodotti TIC, servizi TIC e processi TIC affidate ad organismi di valutazione della conformità accreditati che, sono, comunque, garanzia di valutazioni indipendenti rispetto al livello di resistenza di prodotti TIC e servizi TIC alle minacce di sicurezza cibernetica a beneficio anche dell'utilizzatore finale.

Potrebbe, infatti, sussistere il rischio che i fabbricanti di prodotti TIC e fornitori di servizi TIC, nel miglioramento dei propri prodotti destinati al mercato, investano in maggior misura in servizi di consulenza prestati da fornitori di servizi di sicurezza gestiti, piuttosto che in attività di certificazione prestate, invece, da organismi di valutazione della conformità accreditati, che potrebbero ridurre, quindi, il livello di oggettività sul giudizio di affidabilità di prodotti TIC e servizi TIC immessi sul mercato. Ciò, in considerazione del fatto che i fornitori di servizi di sicurezza gestiti, a differenza degli organismi di valutazione della conformità accreditati indipendenti, prestano un'attività di consulenza commissionata dal fabbricante di prodotti TIC o fornitore di servizi TIC, potendo partecipare al processo di sviluppo, revisione, manutenzione ed erogazione di prodotti TIC e servizi TIC.

2. Conformità del progetto all'interesse nazionale

Le disposizioni contenute nella proposta di regolamento possono ritenersi conformi all'interesse nazionale in quanto in linea con le iniziative poste in essere dal nostro Paese in materia di cybersicurezza.

Inoltre, la certificazione di servizi di sicurezza gestiti ai sensi del regolamento (UE) 2019/881, oltre

a rispondere ad un interesse generale europeo, appare rispondere anche ad interessi nazionali, facilitando la crescita di fornitori di servizi gestiti per l'ambito nazionale.

3. Prospettive negoziali ed eventuali modifiche ritenute necessarie od opportune

La proposta di regolamento è stata pubblicata dalla Commissione europea il 18 aprile 2023 senza il coinvolgimento preventivo dello European Cybersecurity Certification Group (ECCG), che è istituito ai sensi dell'articolo 62 del regolamento (UE) 2019/881 e composto da rappresentanti degli Stati membri con il compito di coadiuvare la stessa Commissione europea nell'elaborazione di politiche in materia di certificazione della cybersicurezza. In occasione della riunione dell'ECCG del 26 maggio 2023, tenutasi ad Atene, diversi Stati membri hanno lamentato il mancato coinvolgimento del Gruppo nella fase di predisposizione della presente proposta che riguarda proprio le sue competenze ed il suo ambito di operatività.

L'avvio del negoziato in Consiglio e in Parlamento europeo dovrebbe essere previsto per settembre 2023. Non è ancora possibile ipotizzare i tempi per la conclusione del negoziato, anche in considerazione delle prossime elezioni europee che si svolgeranno nella primavera del 2024. Al Consiglio il dossier dovrebbe essere assegnato all'*Horizontal Working Party on Cyber Issues* (HWPCI)**,** il gruppo di lavoro orizzontale sulle questioni informatiche (Cyber).

C. Valutazione d'impatto

1. Impatto finanziario

Si evidenzia che per poter procedere ad una compiuta analisi dell'impatto finanziario della proposta è opportuno attenderne i futuri sviluppi negoziali, nonchè l'effettiva adozione da parte della Commissione europea di sistemi europei di certificazione della cybersicurezza, con successivi atti di esecuzione della Commissione europea (articolo 49, paragrafo 7, del regolamento (UE) 2019/881, come sostituito dalla presente proposta) che includano la certificazione di «servizi di sicurezza gestiti».

2. Effetti sull'ordinamento nazionale

Gli emendamenti al regolamento (UE) 2019/881, di cui alla presente proposta di regolamento, richiederanno delle modifiche formali alla norma nazionale di attuazione del regolamento (UE) 2019/881, ovvero il decreto legislativo 3 agosto 2022, n. 123, per introdurvi la nuova categoria di "servizi di sicurezza gestiti".

3. Effetti sulle competenze regionali e delle autonomie locali

La proposta di regolamento non rientra nell'ambito di competenze specifiche regionali o enti locali, riguardando delle competenze attribuite allo Stato dal richiamato decreto legislativo n. 123 del 2022 che ha attuato a livello nazionale il regolamento (UE) 2019/881 ed ha individuato l'Agenzia per la Cybersicurezza Nazionale, ai sensi dell'articolo 5 del decreto-legge 14 giugno 2021, n. 82, quale autorità nazionale per la certificazione della cybersicurezza (articolo 7, comma 1, lettera e), del D.L. n. 82/2021 e articolo 4, comma 1, del d.lgs. n. 123/2022).

4. Effetti sull'organizzazione della pubblica amministrazione

La proposta di regolamento non ha, al momento, effetti sull'organizzazione della P.A. ed in

particolar modo sull'organizzazione dell'Agenzia per la Cybersicurezza Nazionale, quale autorità nazionale di certificazione della cybersicurezza, ai sensi dell'articolo 58 del regolamento (UE) 2019/881. Eventuali effetti potrebbero prodursi con la successiva adozione di sistemi europei di certificazione della cybersicurezza (con atti di esecuzione della Commissione europea ai sensi dell'articolo 49, paragrafo 7, del regolamento (UE) 2019/881, sostituito dalla presente proposta legislativa) che includeranno la certificazione di servizi di sicurezza gestiti, rispetto ai soggetti pubblici che a livello nazionale svolgeranno tali attività.

5. Effetti sulle attività dei cittadini e delle imprese

Dalla certificazione europea di «servizi di sicurezza gestiti» potranno svilupparsi operatori economici certificati in grado di prestare tali servizi a beneficio di imprese. Dall'incremento dei «servizi di sicurezza gestiti» certificati potrebbe, come sopra evidenziato, prodursi una diminuzione della domanda di certificazioni rilasciate dagli organismi di valutazione della conformità indipendenti accreditati ai sensi del regolamento (CE) 765/2008. Ci si attende anche un'apertura maggiore del mercato delle certificazioni con una crescita anche del settore dei servizi di riferimento.

Altro

Si precisa che la proposta nella sua versione originale è suscettibile di essere modificata nel corso del negoziato nell'ambito delle competenti sedi istituzionali europee e che la posizione della delegazione italiane potrà evolvere, agli esiti del coordinamento con le amministrazioni e le parti interessate.