Agenzia per la Cybersicurezza Nazionale

Seguiti Audizione del 23 ottobre u.s. presso la 4ª Commissione (Politiche dell'Unione europea) del Senato della Repubblica – Ulteriori elementi con specifico riferimento alle proposte di regolamento del Parlamento europeo e del Consiglio, COM (2023) 208 in materia di servizi di sicurezza gestiti.

1. Considerazioni dell'Agenzia

Come già ampiamente rappresentato nel corso dell'audizione, si valuta positivamente la proposta di regolamento europeo (COM (2023) 208 in materia di servizi di sicurezza gestiti) in quanto mira ad armonizzare i "servizi di sicurezza gestiti" già diffusi nell'UE, stabilendo dei requisiti generali di qualità e tecnico-organizzativi certificabili ai sensi del regolamento (UE) 2019/881 (c.d. *Cyber Security Act*), riducendo così la frammentazione del mercato interno per quanto riguarda le certificazioni riferite a tali servizi.

Sebbene in fase di elaborazione della proposta non vi è stato l'auspicato e tempestivo coinvolgimento dello *European Cybersecurity Certification Group* (ECCG), in via generale si apprezzano i contenuti della stessa proposta, grazie anche al confronto negoziale attualmente in corso a livello tecnico presso il gruppo di lavoro del Consiglio Ue - *Horizontal Working Party on Cyber Issues* (HWPCI).

Tra le principali questioni oggetto di dibattito e confronto tra gli Stati membri e la Commissione europea, vi è quello che riguarda l'elaborazione dello schema di certificazione, che dovrà avvenire dopo l'entrata in vigore del regolamento attraverso l'adozione di un atto esecutivo, che a sua volta dovrà essere poi attuato a livello nazionale. Al riguardo, si ritiene fondamentale non ammettere la "certificazione dei servizi di sicurezza gestiti" come qualcosa di alternativo e potenzialmente meno sicuro rispetto alla "certificazione di prodotto".

2. Proposte emendative degli Stati membri

L'Italia al momento non ha avanzato proposte di emendamento in maniera ufficiale, ma si è limitata a dare un proprio contributo in termini collaborativi e fattivi al dibattito avviato in sede negoziale, analizzando anche le proposte di altri Stati membri, che poi sono state parzialmente recepite nel testo della proposta da ultimo condivisa dall'*Horizontal Working Party on Cyber Issues* (HWPCI).

In particolare, alcune proposte emendative di altri Stati membri hanno riguardato l'estensione della portata dell'iniziativa a livello:

a. soggettivo, al fine di includere nella certificazione non solo i servizi ma anche i *provider* (Belgio).
   La sola certificazione del servizio non è, infatti, ritenuta sufficiente per raggiungere l'obiettivo desiderato, considerato che nel caso dei fornitori dei servizi di sicurezza gestiti, la sicurezza del servizio e quella dell'organizzazione stessa sono intrinsecamente interconnesse. Al riguardo, viene infatti osservato che il considerando 5, l'articolo 1, comma 5, e il nuovo articolo 51a della proposta di modifica al CSA, fanno riferimento anche a criteri di sicurezza che trascendono il servizio stesso e si concentrano sugli aspetti organizzativi (come il personale e le procedure interne). Nelle valutazioni del Belgio, dunque, tale adeguamento fornirà una base giuridica più solida agli organismi di valutazione della conformità e potrebbe aiutare i fornitori a soddisfare i requisiti di cybersicurezza di cui alla direttiva (UE) 2022/2555 (c.d. NIS 2), considerato che gli stessi rientrano nella categoria dei "settori altamente critici" di cui all'Annesso I;
b. oggettivo, al fine di includere nel processo di certificazione specifici servizi, come quelli correlati al riconoscimento da remoto degli utenti ai quali rilasciare un'identità digitale (Francia).

Tali proposte andranno valutate in sede negoziale anche dal punto di vista di impatto sul mercato.

3. Richiesta di elementi di informazione in merito all'opportunità di "*certificare tutta la filiera e non solo la qualificazione dei gestori dei servizi*".

Il tema non è di facile risoluzione, anche perché andrebbe definito cosa si intende per "filiera", la quale può comprendere:

a. il *provider* del servizio di sicurezza gestito;
b. altri *provider* che erogano in parte (subappalto) il servizio di sicurezza gestito;
c. soggetti terzi che erogano servizi ancillari rispetto al servizio di sicurezza gestito;
d. produttori di strumenti impiegati per l'erogazione del servizio di sicurezza gestito.

La richiamata proposta del Belgio riguarda il solo punto a. Per tutti gli altri, invece, andrebbero identificati requisiti appositi.

In linea generale, quantomeno per quanto riguarda il punto b., si potrebbe ipotizzare una "catena di certificazione", secondo la quale un fornitore di servizi di sicurezza gestiti, certificati a un determinato livello di garanzia, possa avvalersi soltanto di soggetti terzi in possesso dei medesimi requisiti soggettivi.

Tali aspetti potranno essere trattati nel corso della predisposizione dello schema di certificazione e del relativo atto esecutivo come sopra già evidenziato.