Contributo di FASTWEB per le Commissioni riunite Affari costituzionali e Trasporti della Camera dei deputati in relazione all'esame del disegno di legge C. 3161, di conversione in legge del decreto-legge 14 giugno 2021, n. 82 recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"

Rinnovando i ringraziamenti alla Commissioni riunite Affari costituzionali e Trasporti della Camera dei deputati per la possibilità concessa, Fastweb, con la presente memoria scritta, rende le proprie considerazioni e valutazioni in merito alle disposizioni introdotte dal decreto-legge 14 giugno 2021, n. 82, in materia di cybersicurezza ed istituzione dell'Agenzia per la cybersicurezza nazionale.

1. OSSERVAZIONI NEL MERITO DEGLI OBIETTIVI GENERALI

Fastweb guarda con favore al decreto in fase di conversione, volto, nei suoi obiettivi generali, al rafforzamento della resilienza cibernetica del Paese, assicurando il corretto coordinamento tra soggetti pubblici e privati coinvolti in materia di cybersicurezza a livello nazionale, europeo ed internazionale. La completa realizzazione della Strategia Italiana sulla cybersicurezza necessita, infatti, di azioni sempre più comuni e condivise volte al rafforzamento cibernetico di tutto il sistema produttivo, delle pubbliche amministrazioni e dei singoli individui. Questa collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, come ovvio, assume maggior rilievo alla luce della necessità di digitalizzazione e trasformazione digitale da svilupparsi nell'ambito del Piano Nazionale di Ripresa e Resilienza.
Anche per questo motivo, riteniamo particolarmente proficua la possibilità di poter partecipare all'istruttoria delle Commissioni ed al dibattito parlamentare connesso, presentando il punto di vista dell'azienda in merito ad una disciplina – ancorché composita ed eterogenea – volta alla tutela degli interessi strategici del Paese.

2. OSSERVAZIONI NEL MERITO DELLA CHIAREZZA DEL QUADRO NORMATIVO DI RIFERIMENTO E POSSIBILI INTEGRAZIONI

Il decreto-legge 14 giugno 2021, n. 82 rappresenta un ulteriore passaggio volto alla definizione della strategia di cyber-resilienza nazionale, avviata – in un primo momento – con il decreto-legge 25 marzo 2019, n. 22 (c.d. "DL Brexit"), che ha esteso l'ambito di applicazione del c.d. "Golden Power" alle reti di telecomunicazioni, rafforzata dal decreto-legge 21 settembre 2019, n. 105 – c.d. "DL Cyber" – e adesso, da ultimo, in via di completamento con il decreto-legge in esame.

Pare opportuno sottolineare che questa struttura normativa di rango primario, così composta ed articolata, necessiti ancora di una piena attuazione, ad opera di successivi provvedimenti attuativi che, allo stato, non risultano completamente adottati.

Data la complessità della materia in esame e lo stratificarsi di interventi normativi diversi e distanti tra loro nel tempo, la normativa, nella sua interezza, appare poco chiara e di difficile comprensione.

Prova di quanto sopra è costituita, a titolo meramente esemplificativo, dal disposto degli articoli 15 ("*Modificazioni al decreto legislativo NIS*") e 16 ("*Altre modificazioni* ") che apportano modificazioni a circa 6 norme di rango primario e a svariati provvedimenti attuativi, di natura regolamentare.

In questo senso – ed al netto dei vincoli all'attività emendativa del Parlamento nell'ambito della conversione in legge di decreti-legge – auspichiamo che la conversione del decreto possa costituire una prima occasione per armonizzare, coordinare e semplificare la normativa attualmente vigente, restituendo un contesto di riferimento quanto più trasparente possibile, anche attraverso la redazione di un Testo Unico che razionalizzi la disciplina sulla materia, fornendo a tutti gli stakeholder un quadro di riferimento operativo inequivocabile.

Come noto, il Governo sarebbe tenuto a procedere ad una revisione periodica delle normative vigenti, con il precipuo scopo proprio di ridurre il fenomeno della stratificazione e razionalizzando – in questo modo – non solo il lavoro degli interpreti, ma anche quello degli operatori.

In considerazione della particolare rilevanza che, nel recente passato, ha assunto la tutela degli interessi strategici nazionali connessi alla cybersicurezza, auspichiamo che proprio su questa materia si possa procedere alla redazione di un'unica fonte normativa, in luogo delle attuali 3.

Inoltre, sempre in un'ottica di armonizzazione normativa, reputiamo fondamentale prevedere uno snellimento ed una razionalizzazione dei punti di contatto e di interlocuzione tra soggetti privati e autorità pubbliche competenti in materia di cybersicurezza. Il susseguirsi di interventi normativi provenienti da molteplici e diverse fonti di legge nazionali, europee ed internazionali (ad esempio, Direttive NIS, c.d. GDPR, DL Golden Power, DL Cyber, DL Agenzia Cybersecurity) ha contribuito a creare un quadro interlocutorio frastagliato e diversificato. Sarebbe quindi auspicabile identificare un soggetto pubblico nazionale come unico interlocutore in materia di cybersicurezza anche rispetto alle richieste delle varie autorità coinvolte, nazionali, europee ed internazionali.

3. OSSERVAZIONI SULLE TEMPISTICHE DI NOTIFICA GOLDEN POWER

Il decreto in esame reca disposizioni che modificano la disciplina dell'articolo 1-bis, comma 3-bis, del c.d. "DL Golden Power", come modificato dal c.d. DL Brexit, ossia la disciplina dei "*poteri speciali inerenti le reti di comunicazione elettronica a banda larga con tecnologia 5G"*.
Le modifiche introdotte impattano sul processo di notifica previsto nella normativa Golden Power che deve includere obbligatoriamente la comunicazione del Centro di Valutazione e Certificazione Nazionale.

Dall'articolo 16 – che modifica le disposizioni della normativa Golden Power - non risulta chiaro se la valutazione da allegare alla notifica alla Presidenza del Consiglio dei Ministri si riferisca alla Valutazione preliminare del CVCN da effettuarsi entro 45 giorni o entro 60 giorni in casi particolari oppure se l'esito della valutazione debba contenere obbligatoriamente l'esito dei test imposti, che allungherebbe fino oltre i 130 gg i tempi per la conclusione del procedimento.

A nostro avviso può risultare maggiormente efficace prevedere un meccanismo di parallelismo tra la valutazione tecnica e quella politica, allo scopo di contenere i tempi necessari per un riscontro all'operatore nel limite degli (attualmente vigenti) 100 giorni, che comunque rimangono un ordine temporale eccessivamente lungo per l'espletamento degli obblighi collegati al Perimetro di Sicurezza Cibernetica e al Golden Power.

4. ATTIVITA' DI CYBERSICUREZZA PUBBLICO PRIVATO

Infine, come anticipato, desideriamo esprimere un giudizio favorevole nei riguardi di tutte le iniziative che possano coinvolgere soggetti pubblici e privati, in modo da rafforzare e implementare la resilienza

delle strutture e delle attività di cybersicurezza nazionali. In previsione delle strategie di investimento in cybersicurezza delle aziende, auspichiamo che le attività previste dall'articolo 7, comma 1, possano trovare una realizzazione anche attraverso ulteriori atti normativi che permettano una concreta condivisione delle capacità tecnologiche, in modo che possano essere messe a disposizione in termini di capacità progettuali, di piattaforme e di servizi: dal test, al monitoraggio, alla verifica e gestione degli incidenti di cybersicurezza.