Memoria TIM

sul decreto-legge 14 giugno 2021, n. 82 *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale".*

Si riporta di seguito il contributo di TIM in relazione all'esame del disegno di legge C. 3161, di conversione 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"*.

1. Premessa:

L'emergenza epidemiologica ha portato alla luce il ruolo strategico delle infrastrutture e servizi di comunicazione elettronica nello sviluppo degli scenari sociali ed economici del Paese.

La sicurezza delle reti e la conseguente necessità di adottare misure atte a garantirne l'integrità e a tutelare i dati ivi trasmessi è diventata una priorità da garantire.

Per TIM, la sicurezza delle proprie reti e dei dati che vi transitano è da sempre un aspetto di primaria importanza, TIM è impegnata costantemente a garantire la robustezza delle proprie infrastrutture.

L'evoluzione delle tecnologie digitali che si stanno inserendo nelle infrastrutture di telecomunicazioni, con un processo continuo e rapido di aggiornamento, sottopone gli Operatori di telecomunicazioni, a potenziare ulteriormente la propria organizzazione mettendo in campo un processo finalizzato all'applicazione di misure fisiche e logiche (tecniche e organizzative/procedurali – preventive e reattive/di contenimento) che garantiscano efficacia ed efficienza nella gestione proporzionale di scenari di rischio complessi e dinamici.

TIM da sempre collabora attivamente con le istituzioni nazionali ed europee per lo sviluppo di un programma di interventi di attuazione della strategia per la sicurezza cibernetica ed ha applicato tutte le norme vigenti.

In particolare, TIM ha messo in atto quanto specificato dal Decreto del Ministero dello Sviluppo Economico del 12 dicembre 2018, rispondendo agli adempimenti in coerenza con le prescrizioni e i termini temporali. Inoltre, per quanto riguarda le reti 5G, che rientrano nell'ambito di applicazione dei poteri speciali (Golden Power), TIM ha preso parte all'attività di produzione di un risk assessment nazionale 5G, dal quale sono emerse delle indicazioni relative all'identificazione della criticità delle componenti in cui si articola una infrastruttura di rete 5G, a cui hanno seguito le procedure di notifica alle Istituzioni previste per le fasi delle operazioni di approvvigionamento di prodotti di manifattura extra-Europea, includendo le relative analisi dei rischi.

In ultimo si ritiene necessario sottolineare **che l'obiettivo della sicurezza del Paese rappresenta un fine comune e necessita di un processo che richiede un approccio coordinato, basato su un impianto di condizioni e regole chiare:**

- in grado di stabilire un contesto di riferimento in cui sia possibile costruire una prospettiva certa per le decisioni e la pianificazione aziendale (operativa e di business);
- compatibili con le dinamiche temporali stringenti che scandiscono il mercato;
- che seguano un processo ben definito, ispirato agli standard ed alle norme e pratiche internazionali;
- che bilancino in modo sapiente adempimenti ed oneri, per competenza, con incentivi ad operare in modo funzionale al conseguimento dell'obiettivo di interesse comune.

In tal senso TIM condivide pienamente lo spirito del decreto-legge in oggetto, che ha l'obiettivo di fornire un quadro armonico e coordinato nella gestione della sicurezza cibernetica nazionale.

2. Considerazioni sul DL *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale":*

TIM considera positivamente la scelta di costruire un unico punto di riferimento, , per la gestione della sicurezza cibernetica nazionale, identificato nell'Agenzia per la cybersicurezza nazionale.

Come anticipato anche in premessa, in virtù del principio di buon andamento della Pubblica Amministrazione che vuole il rispetto dei criteri di economicità, rapidità, efficacia, efficienza, miglior contemperamento dei vari interessi nell'adempimento dell'attività amministrativa, riteniamo che sia fondamentale avere un approccio coordinato che assicuri una gestione organica del processo e che abbia regole chiare in grado di fornire agli operatori una prevedibilità sulle valutazioni e sui prerequisiti di sicurezza delle reti.

TIM ha seguito e supportato, anche nell'ambito dell'apposito tavolo di lavoro di Confindustria Digitale (di cui si condivide la memoria depositata nel corso dell'audizione relativa al DL in oggetto), l'evoluzione della normativa relativa al Perimetro di Sicurezza Cibernetica e considera positivamente molte delle iniziative, intraprese dal Governo, volta a definire il perimetro di normativo per la gestione della cybersecurity.

Nella considerazione che l'obiettivo perseguito dalle disposizioni urgenti in tema di cyber-sicurezza è anche la razionalizzazione degli interventi in materia, fornendo, allo scopo, regole chiare da seguire per tutti i soggetti iscritti al Perimetro, TIM ritiene che andrebbe approfondito l'aspetto legato alle verifiche da effettuare su un bene ICT da parte del CVCN, allorquando lo stesso asset sia oggetto di notifica al Dipartimento per il Coordinamento Amministrativo della Presidenza del Consiglio dei Ministri in ottemperanza all'obbligo di cui all'articolo 1 -bis del decreto-legge 15 marzo 2012, n. 21 (Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G).

Si potrebbe, infatti, concretizzare uno scenario nel quale, se non venisse attuato un coordinamento tra detti Organismi, con riferimento alla messe in sicurezza di uno stesso asset/ bene ICT potrebbero essere formulate più prescrizioni, differite nel tempo e financo di contenuto tecnico diverso, con conseguenti evidenti difficoltà e costi, da parte della Società, per potervi adempiere compiutamente.

Vogliamo evidenziare che le sfide di digitalizzazione da affrontare nei prossimi anni, che prevedono un cambio radicale nell'utilizzo della tecnologia da parte di cittadini, imprese e

PA potranno essere efficaci e di reale beneficio solo se supportate da infrastrutture resilienti e sicure. In tal senso una trasformazione digitale pervasiva potrà essere garantita solo se associata ad un contesto robusto di cybersicurezza. Pertanto, sarà indispensabile disporre di meccanismi normativi e organizzativi tali da garantire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza nonché lo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza.

Solo attraverso tale meccanismo virtuoso sarà possibile sfruttare a pieno i fondi messi a disposizione dal Piano nazionale di ripresa e resilienza, che prevedono importanti risorse per la transizione digitale del Paese pari al 27% dei fondi stanziati dalla Recovery and Resilience Facility.

In tale contesto tutte le azioni per la digitalizzazione della PA, dall'adozione di un approccio "cloud first" (ad esempio lo sviluppo del Polo Strategico Nazionale) alla razionalizzazione dei processi delle amministrazioni in ottica di interoperabilità, per giungere a soluzioni "once only" sono una priorità a cui TIM vede con estremo favore e per cui apprezziamo che l'importanza della cybersicurezza sia confermata dall'allocazione a questo capitolo di investimento del 10% dell'importo per la digitalizzazione delle PA.

Riteniamo però che la stessa attenzione dovrà essere posta anche all'allocazione degli investimenti in cybersecurity per quanto concerne la trasformazione digitale del tessuto produttivo, superando, ad esempio, nell'investimento per Transizione 4.0, le logiche che avevano inizialmente escluso la cybersicurezza - ma anche altri servizi innovativi - dall'implementazione di Industria 4.0.

Proprio con riferimento al tessuto economico italiano molto deve essere ancora fatto in termini di sensibilizzazione alla cybersicurezza e adozione di quest'ultima nei processi di transizione digitale, fondamentali per garantire una competitività anche a livello internazionale delle nostre imprese. In questo senso auspichiamo che l'Agenzia svolga, un ruolo significativo di sensibilizzazione soprattutto verso l'elevatissimo numero di PMI che rappresentano il tessuto economico del nostro Paese.

In ultimo vogliamo sottolineare che TIM dispone di significative capacità di cyber sicurezza, in termini sia di capacità progettuali, sia di piattaforme, sia di servizi: dal test, alla formazione, al monitoraggio alla gestione degli incidenti, pertanto auspichiamo che possa nascere una proficua collaborazione con l'Agenzia per la cybersicurezza nazionale.