AUDIZIONE ANDREA CAMPORA

- LEONARDO S.P.A.

L'impegno di Leonardo nella cybersicurezza

Leonardo è uno dei principali attori della cybersecurity a livello nazionale ed europeo. Dunque, in Italia l'azienda lavora principalmente con la Pubblica Amministrazione (a esempio, come socio del **Polo Strategico Nazionale)** e coopera con le maggiori infrastrutture critiche, con le utilities e con tutte le grandi realtà che hanno un impatto sulla vita e sull'economia del Paese.
Sul piano europeo, invece, oltre alla realizzazione del **Centro Paneuropeo di Cyber Threat Intelligence per la DG-Connect**, Leonardo partecipa attivamente con la Commissione europea ad organizzazioni che guardano all'innovazione e allo sviluppo e collabora con alcune delle principali università.

Il quadro dell'intervento legislativo alla luce del diritto europeo

Il disegno di legge in esame è ascrivibile alla legislazione europea in materia, una legislazione in continua evoluzione: gli atti adottati negli ultimi anni o in fase di adozione sono numerosi. Basti pensare alla direttiva **NIS2**, al **Cyber Resilience Act** per la resilienza dei prodotti digitali, o al **Cyber Solidarity Act** per creare uno scudo europeo di protezione cyber e infine **all'emendamento al Cyber Security Act** che mira ad ampliare la certificazione da parte delle direttive **NIS** non solo ai prodotti ma anche agli operatori di servizi c.d. "cyber trusted".

La minaccia cyber in numeri e il ruolo dell'AI

A livello mondiale la valutazione economica attuale del danno causato dalla minaccia cyber è tra i 9 e gli 11 mila miliardi di dollari, cifra destinata ad aumentare fino a raggiungere la soglia di 24 mila miliardi nel 2027. Come emerso dal recente report del CLUSIT, in Italia nel 2023 sono stati registrati 310 attacchi gravi (che hanno avuto successo), il 65% in più rispetto al 2022. Per quanto riguarda la spesa in cyber security in Italia, invece, le stime indicano circa lo **0,12% del Pil**, percentuale che classifica l'Italia ultima tra i paesi del G7: gli Stati Uniti spendono più dello 0,3%, Germania e Francia circa lo 0,2%.
L'intelligenza artificiale ha enormemente ampliato le capacità della minaccia cyber in modo asimmetrico - senza dover rispettare alcuna regola – e, quindi, ne ha ampliato l'efficacia. Ciò significa che per contrastarla è necessario che lo Stato sia informato in modo tempestivo, possa governare tutta una serie di informazioni delocalizzate sugli incidenti e possa prendere delle decisioni di facile attuazione, attraverso un apposito sistema di governance.

Il positivo rafforzamento dell'ACN

Alla luce di tali premesse, è particolarmente positivo il rafforzamento dei poteri dell'ACN. L'obbligo di segnalazione di cui all'articolo 1 risponde all'esigenza di avere un punto unico e tempestivo di informazione mentre la possibilità di avere una funzione cyber security e un referente cyber security nella pubblica amministrazione risponde all'esigenza di avere qualcuno in grado di agire e di raccogliere le informazioni.
Allo stesso tempo, attribuire all'ACN il compito e la possibilità di stabilire gli interventi risolutivi significa, inoltre, darle una capacità attuativa estremamente efficace in caso di attacchi o in assenza quando siano evidenti delle vulnerabilità. Altrettanto importante è infine **la previsione di un**

prossimo DPCM con cui l'ACN stabilirà delle norme dei requisiti di cyber security da rispettare e eleverà quella che è la qualità dell'offerta e della proposizione.

Proposte di Elementi Migliorativi

Ci sono alcuni possibili elementi che potrebbero essere migliorativi del testo:

- è importante utilizzare in modo ottimale le risorse, le capacità e le tecnologie delle imprese private per la protezione del paese. Quindi, all'articolo 7, sarebbe opportuno e ugualmente importante prevedere l'avvio di PPP anche nel settore della cybersicurezza. In tale ottica di collaborazione tra settore pubblico e privato, è auspicabile **la creazione di una cyber reserve nazionale**, analogamente a quanto previsto a livello di legislazione europea nell'ambito del regolamento europeo sulla solidarietà in materia di cybersicurezza ("Cyber Solidarity Act"). Per tutelare la sovranità e la sicurezza nazionale, la cyber reserve dovrebbe essere composta da aziende private certificate grazie all'emendamento al Cybersecurity Act per gli MSSP ("trusted providers") e approvate dall'Agenzia per la Cybersicurezza Nazionale. Le aziende che parteciperanno alla cyber reserve nazionale saranno chiamate ad intervenire in caso di crisi per supportare le infrastrutture critiche e la PA in attività di mitigazione degli attacchi e ripristino dei sistemi;

- per garantire il corretto funzionamento della cyber reserve bisognerebbe prevedere un supporto economico adeguato, in modo che le Amministrazioni non limitino al minimo gli interventi correttivi e possano garantirsi servizi di qualità. A tal fine si propone di valutare la costituzione di un fondo dedicato. Investire oggi in cyber security significa anche risparmiare soldi che si devono spendere in caso di attacchi;

- con riferimento all'articolo 10 è fondamentale prevedere che:
  - **a)** la partecipazione ai bandi per l'acquisizione di beni e servizi di cybersicurezza sia **limitata ai soli soggetti "Trusted"** e cioè idonei ad operare su sistemi che concorrono alla tutela degli interessi nazionali strategici (la Francia, per esempio, ha individuato per la protezione delle infrastrutture critiche, un numero di attori "trusted");
  - **b)** il **processo di acquisizione o di ammodernamento di beni e servizi** di cybersicurezza sia condotto con rapidità e flessibilità, consentendo alle Amministrazioni di reagire alle minacce tempestivamente. La minaccia cyber ha una capacità di modificarsi e di evolvere che non è compatibile con quello che è un modello corretto per molte altre ragioni di procurement pubblico "a cascata", con una definizione dei requisiti delle gare e una definizione molto precisa di quello che è al listino. **Un prodotto cyber è obsoleto in pochissimi mesi, quindi il fattore tempo da un lato e una certa flessibilità dall'altro nei modelli di acquisto oggi è vitale per poter essere efficaci in questo tipo di contrasto.**