PROPOSTE EMENDATIVE AL DISEGNO DI LEGGE N. 1717

Audizione presso le Commissioni I e II della Camera dei deputati

Avv. Stefano Mele

Partner presso Gianni & Origoni e Responsabile del Dipartimento Cybersecurity, Privacy & Space Economy Law
Professore a contratto di "Diritto e Politiche del Cyberspazio per la Sicurezza Nazionale" presso la Facoltà di Giurisprudenza dell'Università degli Studi di Foggia

INTRODUZIONE.

La "**Relazione sulla Politica dell'Informazione per la Sicurezza**" del 2024, presentata al Parlamento dalla nostra Intelligence, pone ancora una volta in evidenza – e cito – "*la **centralità del dominio cibernetico quale strumento** preferenziale a cui gli attori ostili fanno ricorso **per il raggiungimento di obiettivi strategici***". La medesima Relazione, inoltre, conferma anche come l'attività svolta dalla nostra Intelligence abbia permesso di rilevare quanto il costante interesse degli attori della minaccia sia "*crescente nei confronti delle **infrastrutture digitali dei soggetti pubblici, con particolare attenzione verso quelle riferibili alle Amministrazioni Centrali dello Stato e agli Istituti e Agenzie nazionali***" con una percentuale sul totale degli attacchi rilevanti a danno della PA di ben il 65%. Nel 2022, si è attestata sul 62%.

In una frase: **la nostra Pubblica Amministrazione è costantemente soggetta ad attacchi *cyber***.

PROPOSTE EMENDATIVE.

Il Disegno di Legge inerente alle "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", deve considerarsi, quindi, centrato su un **tema realmente utile e concreto per la sicurezza del nostro Paese**.

Ciò premesso, per porgere alla Vostra cortese attenzione il mio contributo scientifico sul tema, considerati i tempi a mia disposizione, mi limiterò ad individuare sinteticamente dei punti di attenzione per migliorare il testo del Disegno di Legge, rimandando ad ulteriori e successivi approfondimenti. In particolare:

- In via introduttiva, ritengo importante segnalare che l'Italia, così come tutti gli altri Paesi membri dell'UE, si appresta a dare attuazione, entro ottobre 2024, alla Direttiva NIS2. Questa Direttiva prevede che la pubblica amministrazione sia inclusa tra i soggetti destinatari di precisi e stringenti obblighi di cybersicurezza, tra cui spiccano proprio azioni molto simili a quelle oggi analizzate nel Disegno di Legge. L'attuale Disegno di Legge, infatti, sembra porsi quasi come una "anticipazione" della Direttiva NIS2. Pongo, allora, alla Vostra cortese attenzione **l'esigenza di raccordare quanto in discussione oggi con gli obblighi ormai imminenti della Direttiva NIS2, al fine di evitare eventuali sovrapposizioni o addirittura duplicazioni**. Considerata la forte – e importantissima – esigenza di cybersicurezza soprattutto per la pubblica amministrazione, si potrebbe decidere, infatti, di **accelerare il più possibile l'attuazione della Direttiva NIS2**.

- Il Disegno di Legge, all'art. 1, comma 1, chiarisce subito di rivolgere la propria attenzione alle pubbliche amministrazioni centrali, alle regioni e alle province autonome di Trento e Bolzano, ai comuni con popolazione superiore a 100.000 abitanti e, comunque, ai comuni capoluoghi di regione, nonché alle società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti e le aziende sanitarie locali.
  A questi soggetti, l'art. 6, comma 1, richiede – a mio avviso correttamente – di **identificare una struttura che si occupi di cybersicurezza**. Considerato che la norma si rivolge ad un ampio spettro di pubbliche amministrazioni, che, nel corso del tempo, non sempre hanno avuto la possibilità e soprattutto la sensibilità di sviluppare le opportune **strutture per la *cybersecurity***, ma considerata l'estrema utilità e anzi l'estrema urgenza di gestire correttamente questo tema, il mio suggerimento è quello di **concedere un periodo di tempo (anche solo di 6/12 mesi) per l'attuazione di questa richiesta**. Ciò anche al fine di permettere a questi soggetti di sfruttare a pieno i **50 milioni messi a disposizione dall'Agenzia per la Cybersicurezza Nazionale (ACN)** attraverso il bando per "***Interventi di potenziamento della resilienza cyber – PA***", la cui scadenza è stata prorogata proprio ieri.

- Sempre in relazione a questi soggetti, all'art. 6, comma 2, viene richiesto – giustamente – di identificare all'interno della struttura di *cybersecurity* un "***referente per la cybersicurezza, individuato in ragione delle qualità professionalità possedute***". Considerato che la norma si rivolge ad un ampio spettro di pubbliche amministrazioni, che, nel corso del tempo, non sempre hanno avuto la possibilità e soprattutto la sensibilità di sviluppare le opportune competenze su questo tema, **appare opportuno concedere il "giusto tempo" per individuare (e in alcuni casi formare) questi soggetti**. Ciò, al fine di evitare che questa importante responsabilità venga data ad un professionista non realmente preparato e competente per questo incarico. Perciò, **l'auspicio è che venga previsto un periodo di tempo (anche solo di 6/12 mesi) in cui sia possibile far supportare questa figura interna anche da consulenti esterni**, fermo restando la indiscutibile utilità che questa figura esista e che sia interna alla struttura della PA.
  Per di più, ritengo importante anche che il nuovo testo del Disegno di Legge **delinei in maniera più precisa quali competenze questi soggetti debbano avere sul piano professionale**, in modo da poter garantire che il criterio delle "*qualità professionalità possedute*" dal futuro Referente per la cybersicurezza nelle PA non sia così ampio e generico da farvi rientrare anche soggetti che abbiano solo una infarinatura della materia. Ciò, infatti, creerebbe una condizione di finta sicurezza, rendendo così questa ottima intuizione del legislatore quasi come una "lettera morta".

- Sempre per i soggetti individuati nell'art. 1, comma 1, del Disegno di Legge si evidenzia come l'attuale testo del Disegno di Legge si rivolga esclusivamente alle società di trasporto pubblico urbano con bacino di utenza superiore a 100.000 abitanti. Se è correttamente avvertita questa esigenza per le società che erogano un servizio urbano, **si suggerisce di includere anche quelle del trasporto extra-urbano**.

- In linea generale, si evidenziano richieste applicative in materia di *cybersecurity* a favore della pubblica amministrazione decisamente onerose, seppur correttissime. **Prevedere un lasso di tempo per la loro attuazione**, che al momento manca nel testo del Disegno di Legge, potrebbe essere una mossa anzitutto di buon senso.

- Il Disegno di Legge, all'art. 9, prevede anche una novella delle disposizioni in materia di personale dell'Agenzia per la Cybersicurezza Nazionale (ACN). L'esigenza primaria, infatti, è quella di **continuare ad incentivare i migliori giovani professionisti a scegliere l'ACN** e a restare all'interno di questa nostra importantissima struttura. Ritengo, quindi, che questo Disegno di Legge – e in particolar modo il suo art. 9 – siano la migliore occasione per muoversi in questa direzione, introducendo, ad esempio, ulteriori incentivi, come quello di **garantire al personale distaccato presso l'ACN il mantenimento del proprio ruolo all'interno dell'amministrazione di origine** (come avviene per il settore Intelligence).

- Considerata l'attenzione che il nostro legislatore correttamente pone al tema delle estorsioni digitali attraverso **attacchi *ransomware***, suggerisco di cogliere questa opportunità anche per normare i casi limite – e ovviamente denegati – in cui le nostre società si vedano costrette a pagare il riscatto perché in uno stato comprovato di necessità. Potrebbe risultare molto utile **imporre un obbligo di notifica quantomeno all'Agenzia per la Cybersicurezza Nazionale (ACN) dell'azione di pagamento del riscatto**, in modo da avere una reale e concreta contezza del fenomeno e far emergere i casi di sommerso. Ciò sarebbe in linea, peraltro, con quanto il CISA americano sta per chiedere alle proprie società.

CENNI BIOGRAFICI DELL'AUTORE.

Stefano Mele è *Partner* presso lo Studio legale Gianni & Origoni dove è il Responsabile del Dipartimento di Cybersecurity & Space Law e co-Responsabile del Dipartimento Privacy.

È, inoltre, il Presidente dell'*Autorità per le Tecnologie dell'Informazione e della Comunicazione* ("Autorità ICT") della Repubblica di San Marino.

È membro del *Regulatory and Governance Committee* del Consiglio di amministrazione di NEOM.

È Professore a contratto di "*Diritto e Politiche del Ciberspazio per la Sicurezza Nazionale*" presso la Facoltà di Scienze Giuridiche della Sicurezza dell'Università degli Studi di Foggia, nonché *Academic Fellow* della cattedra di *Cybersecurity* presso il Dipartimento di Studi Giuridici dell'Università Bocconi e collaboratore presso le cattedre di Informatica Giuridica e Informatica Giuridica Avanzata della Facoltà di Giurisprudenza dell'Università degli Studi di Milano.

È membro del Comitato Etico-Giuridico dell'Arma dei Carabinieri.

È membro del Consiglio Direttivo e Presidente della Commissione Sicurezza Cibernetica del Comitato Atlantico Italiano, oltre che Presidente del "*Gruppo di lavoro sulla Cybersecurity*" della Camera di Commercio americana in Italia (AMCHAM).

Nel 2020, è stato invitato a partecipare al prestigioso International Visitors Leadership Program (IVLP) del Dipartimento di Stato americano. Infine, nel 2014, la rivista americana Forbes lo ha inserito tra i 20 migliori *Cyber Policy Experts* al mondo da seguire in Rete.