Audizione informale per il disegno di legge in materia di

«Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)

Camera dei Deputati, Commissioni riunite I e II

28 marzo 2024

di

Erik Longo

Università degli Studi di Firenze

1. Introduzione

Ringrazio i Presidenti e gli onorevoli membri delle Commissioni I e II per il gentile invito a prendere parte a questo ciclo di audizioni sul disegno di legge in materia di «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717).

Le mie osservazioni provengono dalla lettura del testo del disegno di legge e dal Dossier che è stato preparato dai servizi studi congiunti di Camera e Senato. Ho avuto modo di leggere alcune delle memorie depositate e ascoltare le ricche audizioni svolte fino ad ora.

Il primo dato che vorrei sottolineare, e che rappresenta un punto di partenza necessario per ragionare sul disegno di legge odierno, è che ci troviamo in un momento del tutto particolare della storia, nel quale affrontare nuove norme sulla cybersicurezza rappresenta una decisione politica che attiene alla sostanza della sovranità dello Stato italiano, tanto nella sua dimensione interna quanto nella sua dimensione esterna.

La cybersicurezza oggi interessa tutti e non solo gli esperti. Non si tratta più solo di una questione legata all'intelligence o alla messa in sicurezza di alcuni dispositivi che possono essere infettati da "malattie" informatiche. La vita digitale ci espone in ogni momento a nuove minacce dovute tanto a errori quanto a comportamenti intenzionalmente malevoli.

L'esigenza di protezione dal rischio di un attacco informatico e dai danni che ne possono derivare, riassunta nel termine "cyber-resilienza", sta spingendo molti paesi del mondo a concepire in maniera diversa la sicurezza stessa, e quindi le dinamiche di potere che a essa si riferiscono.

L'ultimo rapporto Clusit riporta che dal 2018 abbiamo assistito a un aumento del 61,5% a livello mondiale e del 300% nel nostro Paese di attacchi arrivati a buon fine. Gli attacchi ransomware sono cresciuti del 41% nel 2022. Anche gli attacchi via e-mail, compreso il phishing, sono aumentati del 48% nel 2022. Gli attacchi hanno iniziato a concentrarsi anche sull'interruzione delle catene di approvvigionamento, già perturbate a seguito della pandemia e ancor più dopo l'inizio della guerra in Ucraina.

Il costo di questi incidenti sta salendo alle stelle. Uno studio del 2020 del *Joint Research Center* dell'UE ha stimato che il costo globale della criminalità informatica ha raggiunto una cifra che supera i 5 trilioni di euro, rispetto ai 2,7 trilioni di euro del 2015. La stima per il 2025 è di 10,5 trilioni di dollari. Il costo medio globale di una violazione dei dati nel 2022 è stato stimato in 4,35 milioni

di dollari. L'agenzia europea ENISA evidenzia che aziende e istituzioni europee spendono il 41% in meno per la sicurezza informatica rispetto agli Stati Uniti.

2. Introdurre la cultura della cybersicurezza

In tale ottica diviene essenziale non solo garantire servizi ed evitare danni ma anche diffondere il più possibile la cultura della cybersicurezza. È quanto mai opportuno promuovere una profonda consapevolezza in tale materia, sottolineando l'importanza cruciale che le minacce digitali assumono nella salvaguardia degli interessi strategici della nazione e nell'incolumità del tessuto produttivo, con un focus particolare sulle vulnerabilità che interessano le amministrazioni, da un lato, e le piccole e medie imprese, dall'altro.

Al fine di elevare il livello di sicurezza informatica e di assicurare una resilienza ottimale di fronte alle minacce cibernetiche, si rende necessario accompagnare norme che impongono obblighi alla predisposizione di strumenti che consentono agli enti e alle imprese di mappare le proprie vulnerabilità e di conoscere da dove possono venire le minacce, con l'obiettivo di fornire una guida concreta per la prevenzione, il rilevamento precoce, la risposta efficace e la ripresa rapida in caso di attacchi informatici. La realizzazione di un simile paradigma di sicurezza richiede un impegno congiunto e coordinato tra gli attori pubblici e privati, un continuo aggiornamento tecnologico e formativo, nonché una costante vigilanza e adattamento alle evoluzioni del panorama delle minacce cibernetiche.

Questo disegno di legge meritoriamente cerca di rafforzare tanto la risposta penale alle minacce alla sicurezza informatica quanto la resilienza della pubblica amministrazione, anticipando e in un certo qual modo mettendo

un "punto fermo" nazionale prima della attuazione della Direttiva 2022/2555 c.d. NIS 2. Come si legge nell'art. 6 della Direttiva, le nuove norme si applicano solo agli enti della pubblica amministrazione a livello centrale. Sono poi gli Stati membri a decidere se estenderle agli enti anche a livello regionale e locale. I problemi di coordinamento delle norme odierne con l'attuazione della NIS mi paiono il problema più rilevante di questo disegno di legge; un problema di fondo che può minare l'efficacia e il risultato sperato dal legislatore. A questo fine, il testo che segue proverà a fornire un quadro composto di tre considerazioni generali e poi tre commenti puntuali.

3. Considerazioni generali

La *prima* osservazione generale attiene alle norme repressive dei fenomeni criminosi. Sono state già svolte molte considerazioni sul punto. Mi limito solo a sottolineare, come è stato già fatto da altri, che la deterrenza sanzionatoria non sempre colpisce nel segno. Semmai essa indica la riconosciuta insidiosità di tali reati e la correlata aggressione a beni giuridici di preminente interesse nella scala costituzionale dei valori. Eviterei di limitarsi ad aumentare le pene senza farne un'occasione per intervenire sui potenziali punti deboli della disciplina, evidenziati da molto tempo da parte della dottrina (anche ultimamente con riguardo al recepimento della Direttiva 2013/40/Ue).

Aggiungo che oramai, data la rilevanza di questi fenomeni e la necessità di realizzare una seria lotta a tali condotte, la scelta del legislatore di inserire le fattispecie secondo una logica di "gemmazione", collocandole a latere di disposizioni già esistenti sulla base del criterio del bene giuridico tutelato, ha determinato un quadro regolatorio troppo frammentato e discontinuo, anche per le continue modifiche imposte dal progresso tecnologico.

Il legislatore dovrebbe perciò utilizzare questo momento per una sistematizzazione delle fattispecie in oggetto evitando di limitarsi a un maquillage del testo codicistico.

La *seconda* considerazione generale riguarda il fatto che sul versante della "resilienza" ci sono una serie di norme di difficile attuazione pratica dovuta a una mancanza di capacità amministrativa e di risorse sia nel breve periodo (nonostante il PNRR) sia (soprattutto) nel lungo periodo.

Il tema è stato ricordato già in altre audizioni. Comprendo che il problema principale per il decisore politico sia dove investire e come spendere in modo efficiente il denaro pubblico ma non dobbiamo dimenticare che nessuna norma, neanche quelle penali, sono a costo zero.

Nel caso di specie, l'introduzione di un "responsabile" o "referente" per la Cybersicurezza negli enti indicati all'art. 1 dimostra una notevole attenzione alle nuove sfide presentate dalla cybersicurezza. Peccato però che la semplice presenza di figure di riferimento, peraltro in assenza di una chiara definizione del loro livello di inquadramento, non appare sufficiente a garantire i risultati.

È fondamentale che il legislatore, oltre a introdurre novità normative in merito, indichi all'Agenzia per la cybersicurezza nazionale di lavorare a stretto contatto con le nuove figure di responsabile o referente che saranno presenti nelle varie amministrazioni, per garantire che i compiti pianificati siano effettivamente realizzati e che vi sia un chiaro processo di monitoraggio e valutazione dei risultati ottenuti, affiancandoli nell'implementazione di strategie operative e di procedure. In coerenza con l'obiettivo garantire un livello elevato di cybersicurezza, vista la natura trasversale e pervasiva della stessa rispetto alla ormai totalità dei servizi di funzionamento delle amministrazioni, ai processi digitalizzati e ai servizi erogati verso soggetti terzi, sarebbe opportuno adottare misure in grado di incidere efficacemente e

tempestivamente, ad esempio prevedendo che il responsabile o referente per la cybersicurezza esprima pareri sugli atti dell'ente incidenti sulle sue aree di competenza e possa pure emanare linee guida e raccomandazioni interne.

Inoltre, se il disegno di legge pone maggiormente l'accento sulla risposta e l'apparato sanzionatorio in caso di attacchi e minacce informatiche, è altresì importante rivolgere l'attenzione alla prevenzione di tali attacchi, con miglioramenti non solo delle regole giuridiche ma anche con un impegno costante nella formazione e aggiornamento delle competenze di tutto il personale della pubblica amministrazione.

La *terza* considerazione attiene allo scenario che si apre di fronte a noi sul piano normativo nei prossimi mesi. Questo disegno di legge anticipa ma dovrà necessariamente coordinarsi con le norme che verranno approvate dal Governo con decreto legislativo per il recepimento della NIS 2. Penso che immaginarsi il contenuto del disegno di legge oggi in discussione senza avere chiaro o aver esplicitato cosa accadrà su quel fronte sia non corretto. Offro sul punto due considerazioni tecniche. La NIS 2 realizza su tanti fronti un cambiamento di prospettiva rispetto al passato, sia nei termini dei soggetti sia nei termini degli strumenti.

Una delle chiavi dell'intervento europeo diviene oggi il sistema di "certificazioni" per la cybersicurezza sul quale siamo chiamati a fare un passo avanti nei prossimi anni. Non è un caso che proprio sul punto è in atto una revisione del Regolamento denominato "EU Cybersecurity Act". Scrivere queste regole senza avere chiaro come si risolverà dall'altra parte il meccanismo certificatorio non aiuta.

L'altra considerazione tecnica mi riporta indietro alla deterrenza penale. Le norme del disegno di legge sul punto andrebbero completate con le regole sul c.d. *ethical hacking* e le forme di garanzia di soggetti che già oggi sono

essenziali per la filiera della prevenzione dei reati informatici. La NIS 2 cerca infatti di incoraggiare pratiche coordinate di *vulnerability disclosure*, invitando sia figure esperte sia *ethical hackers* a segnalare le vulnerabilità di prodotti e sistemi, in modo da consentire di diagnosticarle e porvi rimedio prima che vengano divulgate e abusate da terzi. A tal fine l'ENISA sarebbe tenuta a sviluppare e mantenere un registro europeo delle vulnerabilità per consentire ai settori essenziali e importanti, nonché ai loro fornitori di reti e sistemi informativi, di registrare e divulgare le vulnerabilità nei prodotti o nei servizi ICT.

4. Commenti puntuali

Nel tempo che rimane vorrei provare a offrire alla vostra discussione tre commenti più puntuali relative al settore locale e regionale interessato dal Capo I del disegno di legge odierno.

Il *primo* commento riguarda la filosofia di fondo di questi interventi. La cybersicurezza si genera grazie a processi e non solo per adempimenti. La garanzia della resilienza dei sistemi non avviene semplicemente imponendo un onere di notifica e la individuazione di un responsabile unico per ente sul punto. La prima cosa che occorrerebbe capire è quale livello di "maturità della cybersicurezza" hanno gli enti ai quali tali disposizioni si riferiscono. La filosofia dell'intervento legislativo dovrebbe garantire l'aumento dei livelli di consapevolezza e un più pronto riconoscimento dei fattori di rischio, permettendo uno sviluppo proattivo e preventivo della sicurezza informatica.

Mi immagino perciò che si debba aggiungere una norma che vada concretamente a chiedere alle amministrazioni di essere più consapevoli dei fattori di rischio. Per intenderne l'importanza e comprendere come scriverla, si

può vedere cosa prevede il Regolamento (UE, Euratom) 2023/2048 che stabilisce misure per un livello comune elevato di cybersicurezza nelle istituzioni dell'Unione. Per garantire la segnalazione e la notifica occorrono "misure di valutazione e gestione" dei rischi definite anche in "piani per la cybersicurezza". Gli enti menzionati nell'articolo 1 del disegno di legge, perciò, devono essere prima di tutto obbligati ad attivare misure di rilevamento e gestione dei rischi e, nel caso di violazione di legge, dovranno essere sanzionati anche per questo (oltre che per gli eventuali incidenti).

Qualcuno potrebbe farmi notare che si tratta della parte di attuazione della NIS 2, ma allora occorrerebbe precisare anche nel presente disegno di legge che le norme rivolte a rafforzare la cybersicurezza nazionale avranno un necessario completamento nella fase di recepimento della direttiva. Altrimenti, per il tenore delle disposizioni oggi al vostro esame tali obblighi rischiano di rimanere lettera morta o, peggio, di paralizzare i decisori, tanto a livello locale in fase di adempimento quanto a livello nazionale in sede di verifica dell'adempimento stesso.

Il *secondo* commento riguarda il fatto la cybersicurezza – per usare un'espressione gergale – "si genera insieme" attraverso un quadro conoscitivo chiaro. Nel disegno di legge è dato per scontato che per risolvere i possibili incidenti e garantire la resilienza occorrono soggetti e formule che realizzino una risposta coordinata. È quanto emerge sia nella NIS 2 con riguardo all'EU-CyCLONe e il NIS Cooperation Group sia con riguardo all'emanando regolamento "EU Cybersolidarity Act" che introduce un meccanismo denominato "European Cybersecurity Alert System".

Per questo credo che le norme oggi al vostro esame siano mancanti di un riferimento necessario sia a un meccanismo che per l'Italia si occupi di coordinare la risposta agli incidenti sia della creazione obbligatoria di strutture

decentrate che in alcune regioni oggi sono già presenti o stanno per essere attivate di risposta coordinata agli incidenti. Parlo chiaramente dei SOC e della rete nazionale degli CSIRT creati sulla base delle linee guida ACN, i quali realizzano collaborazioni con lo CSIRT Italia per la preparazione e il supporto alla gestione e risposta a incidenti informatici.

Se davvero si vuole imporre agli enti locali e regionali vincoli in materia di cybersicurezza, occorre aiutarli a realizzare effettivamente la resilienza cibernetica indicando una strada concreta per realizzare tale obiettivo. Il modello CSIRT è l'ambito privilegiato sia per identificare i problemi e poi offrire una risposta coordinata agli incidenti informatici sia per realizzare uno scambio di buone pratiche e incentivare il rispetto delle norme.

In tale senso, credo che il referente per la cybersicurezza debba essere in contatto con i costituiti o costituendi CSIRT costituiti nella propria regione, i quali anche avvalendosi delle in-house regionali e comunali, dovranno vigilare e riportare immediatamente all'ACN ogni incidente, come pure creare un ecosistema innovativo in rete che generi nuova conoscenza sui problemi e le soluzioni (con apertura e contaminazione tra pubblici e privato).

Anche qui potreste ricordarmi che tali norme rientrano nell'attuazione della NIS 2, ma ribadisco che allora ci vuole un coordinamento tra le norme attuali e le emanande disposizioni del decreto legislativo di attuazione.

Il *terzo* e ultimo commento attiene alla realizzazione amministrativa delle esigenze poste dai soggetti che devono gestire a livello locale la cybersicurezza. Stiamo andando incontro a una stagione nella quale sarà molto difficile, soprattutto per via dell'impiego massiccio delle IA, realizzare una efficace resilienza cyber. Gli attacchi oggi sono divenuti più numerosi e più sofisticati.

A questo proposito, propongo di trovare la via per introdurre nell'art. 10 del disegno di legge un riferimento all'articolo 75 del nuovo codice dei

contratti, d.lgs. n. 36/2023, attraverso l'incentivo di forme di "Partenariato per l'innovazione". Dobbiamo immaginare che, per dotarsi di servizi informatici all'avanguardia, i soggetti pubblici – soprattutto di grandi dimensioni – dovranno non solo rivolgersi al mercato dei servizi già esistenti e consolidati ma anche approvvigionarsi di servizi innovativi da costruire insieme e in coordinamento con aziende operanti in tale settore. In questo senso, il partenariato per l'innovazione – come è già sostenuto dalla dottrina – potrebbe essere tanto una soluzione da incentivare quanto un possibile volano di crescita economica per tante piccole e medie imprese, come ad esempio quelle nate a partire da *spin-off* universitari.