Memoria sul 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”

Camera dei deputati

IX Commissione Trasporti, Poste e Telecomunicazioni

30/07/2021 Fabio Mulazzani, PhD

Introduzione

La correlazione tra processi di business e *Information Technologies* (IT) è diventato da tempo un legame imprescindibile per il raggiungimento degli obiettivi di crescita, se non di mantenimento delle posizioni conquistate in un mercato fluido e in rapida evoluzione. Contestualmente, è stata registrata l'accresciuta esposizione a minacce cibernetiche e con essa la necessità di sviluppare tempestivamente adeguate forme di protezione.

Il 6 luglio 2016 veniva emanata la direttiva UE 2016/1148 (c.d. direttiva NIS "*Network and Information Secuirty*"), recepita in Italia con decreto legislativo n.65 del 18 maggio 2018, con lo scopo di incrementare il livello comune di sicurezza dell'Unione Europea. In considerazione dell'aumento senza precedenti del livello di digitalizzazione registrato negli ultimi anni, e ancor di più nel periodo di pandemia da COVID-19, il 16 dicembre 2020 è stato avviato un processo di revisione della summenzionata direttiva per definire una nuova e aggiornata versione (cd. direttiva NIS 2). Le novità previste nell'approvanda direttiva NIS 2 sono sintetizzabili in:

- Maggiori capacità - dovranno essere implementate adeguate misure per la supervisione e coercizione. Dovranno inoltre essere previste sanzioni amministrative per le inosservanze alle norme di cybersecurity;
- Cooperazione – dovrà essere assicurato maggiore scambio di informazioni, coordinamento nella divulgazione della scoperta di nuove vulnerabilità, e l'istituzione di una struttura per il coordinamento di incidenti di cybersecurity di grandi dimensioni;
- Gestione dei rischi – dovranno essere definite delle misure da implementare per il rafforzamento dei requisiti di cybersecurity, ivi inclusa la catena di approvvigionamento. Dovranno inoltre essere semplificate le procedure per la comunicazione di incidenti di cybersecurity;
- Settori considerati – verranno inclusi un maggiore numero di settori e servizi da considerarsi come essenziali oppure importanti.

In Italia, già dal 2019, con decreto-legge 105 e successive modifiche ed integrazioni, veniva previsto un incremento di attenzione alla cybersecurity delle amministrazioni pubbliche, degli enti e degli operatori nazionali pubblici e privati, attraverso l'istituzione del perimetro di sicurezza nazionale cibernetica.

In questo contesto, il decreto-legge 14 giugno 2021, n. 82, per quanto figlio di una situazione emergenziale, costituisce un pilastro fondamentale nell'incremento del livello di maturità della strategia nazionale di cyber-resilienza. Nel definire l'architettura nazionale della cybersecurity, e istituendo l'Agenzia per la cybersicurezza nazionale, il D.L. 82 stabilisce la cornice di governance e operativa necessaria a garantire il raggiungimento tempestivo ed efficace degli obiettivi prefissati, talvolta anticipando i dettami introdotti nella bozza della NIS 2.

Osservazioni

L'esame del disegno di legge in questione è un momento di riflessione e formalizzazione delle opportunità di affinamento della normativa al fine di rispondere a prevedibili necessità strategico-operative. Di seguito è rappresentata una disamina di quelle identificate dallo scrivente.

1) Comitato Interministeriale per la cybersicurezza

   L'articolo 4 istituisce, presso la Presidenza del Consiglio dei ministri, il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

   Si valuti l'opportunità di sovraordinare l'attività di cyber-sorveglianza del CIC rispetto a tutti i progetti in corso, anche a quelli di competenza del Comitato interministeriale per la transizione digitale (CITD).

   Questa misura è orientata a mitigare possibili conflitti di competenza tra comitati, e a garantire che gli aspetti di cybersicurezza vengano considerati come elemento guida di ogni progetto tecnologico-digitale e non un elemento a complemento.

   Inoltre, per quanto il CITD abbia competenza in merito alle attività di coordinamento e monitoraggio di iniziative per lo sviluppo e la diffusione delle tecnologie emergenti dell'intelligenza artificiale, dell'internet delle cose (IoT) e della *blockchain*, si valuti l'opportunità di attribuire la competenza esclusiva al CIC in merito alle tecnologie quantistiche (es. crittografia post-quantistica e quantum distributed ledgers).

   Questa misura è orientata a garantire un'attenzione strategica ad un argomento, le tecnologie quantistiche, che assieme all'IoT e al blockchain è considerato da ENISA (l'agenzia europea per la cybersicurezza) come emergenti e quindi soggetta a rischi di magnitudo significativa.

2) Agenzia per la cybersicurezza nazionale

   L'articolo 5 istituisce l'Agenzia per la cybersicurezza nazionale a tutela degli interessi nazionali nel campo della cybersicurezza. Il successivo articolo 7 definisce le funzioni e compiti dell'Agenzia stabilendo che la stessa promuova "la realizzazione di azioni comuni dirette ad assicurare la sicurezza e resilienza cibernetica per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni […]".

   Una tipologia atipica di pubblica amministrazione sono gli organismi internazionali e le missioni speciali. L'Italia ospita diverse sedi e articolazioni periferiche di detti organismi e con questi intrattiene rapporti così come stabilito in apposti accordi.

   Fatto salvo quanto previsto dai protocolli sui privilegi ed immunità riservato ai summenzionati organismi, si valuti l'opportunità di consentire all'Agenzia di stipulare appositi accordi per l'inclusione degli organismi internazionali tra i fruitori dei servizi offerti dall'Agenzia a similitudine di una pubblica amministrazione italiana.

   Questa misura è orientata ad estendere all'ambito cibernetico la protezione che le competenti autorità italiane già garantiscono a livello fisico agli organismi internazionali presenti in Italia.

3) L'Agenzia quale Autorità nazionale di certificazione della cybersicurezza

   L'articolo 7 (comma 5) individua l'Agenzia quale Autorità nazionale di certificazione della cybersecurity, organismo previsto dal regolamento (UE) 2019/881.

La certificazione di prodotti, servizi, processi delle tecnologie dell'informazione è una disciplina destinata ad aumentare la sua rilevanza per il raggiungimento dei più alti obiettivi qualitativi di cybersicurezza. In un mercato europeo doverosamente aperto ed interconnesso, potrebbero essere immessi in Italia prodotti o servizi formalmente certificati in altri stati membri. Per quanto il principio di "fiducia" (cd. *Trust*) sia un elemento portante delle politiche comunitarie, nell'ambito della cybersicurezza deve essere adottato, ove necessario, il principio dalla "fiducia zero" (cd. *Zero Trust*).

Si valuti l'opportunità di conferire all'Agenzia la funzione di riconoscere l'equipollenza in Italia di certificazioni su prodotti, servizi o processi rilasciate da Autorità di stati terzi.

Questa misura è orientata a rafforzare le misure di controllo e assicurare il loro allineamento non soltanto ai requisiti fondamentali della norma internazionale o europea di riferimento ma anche ad eventuali più stringenti requisiti nazionali.

4) Il personale dell'Agenzia

L'articolo 12 dispone che la disciplina del personale addetto all'Agenzia sia stabilita in apposito regolamento. Detto regolamento, tra l'altro, definisce l'ordinamento e il reclutamento del personale.

In un mercato del lavoro fortemente aperto e globale, molte delle migliori professionalità nell'ambito cibernetico sono già state reclutate al di fuori dell'Italia o comunque a condizioni molto vantaggiose come quelle offerte da organismi internazionali.

Si valuti l'opportunità d'identificare modalità di reclutamento idonee e ad-hoc che possano incrementare la possibilità di assunzione dei profili sopra descritti (a similitudine della cd. Legge per il "rientro dei cervelli").

Conclusioni

La definizione dell'architettura nazionale e l'istituzione dell'Agenzia per la cybersicurezza nazionale costituiscono un primo ma fondamentale passo verso la protezione degli interessi nazionali nella dimensione cibernetica.

Le osservazioni presentate in questo documento vogliono contribuire ad accendere l'attenzione su tematiche che, qualora analizzate e approcciate in maniera strutturale, possono colmare taluni *vulnus* strategico-operativi della norma stessa.

La tempistica di implementazione della normativa diventa un fattore critico per il raggiungimento degli obiettivi prefissati in un contesto globale imprevedibile e volatile. Sarebbe pertanto opportuno aumentare la dotazione del capitolo di bilancio dedicato all'Agenzia ovvero raggiungere in un più ristretto lasso di tempo il livello di finanziamento previsto a regime dal 2027.

La cybersicurezza necessita sia di un supporto normativo, come quello offerto dal DDL oggetto della presente memoria, ma anche e soprattutto di un profondo cambiamento culturale che interessi, non solo i settori inclusivi dei soggetti essenziali e importanti, ma di tutta la società.