MEMORIA SCRITTA IN RISPOSTA ALLA CONVOCAZIONE PER

Audizione informale presso la

IX COMMISSIONE TRASPORTI, POSTE E TELECOMUNICAZIONE

della Camera dei Deputati

nell'ambito dell'esame dello schema di decreto legislativo di "Recepimento della direttiva (UE) 2022/2555 del Parlamento europeo relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2) - ***Atto del Governo n. 164***

Lunedi 15 luglio 2024

Premessa

La sicurezza informatica è ormai un tema ineludibile per tutte le Pubbliche Amministrazioni, di qualunque dimensione e livello amministrativo: il progressivo intensificarsi di attacchi di diversa natura, che siano finalizzati alla messa fuori uso dei sistemi informativi o all'estrazione fraudolenta di dati, rende ineludibile un rafforzamento delle difese cibernetiche, da attuarsi a livello regolamentare e, conseguentemente, operativo a livello di singolo ente.

Il tema, di conseguenza, assume centralità anche per i Comuni, le loro forme associate e le Città metropolitane che, pur gestendo dati i quali, secondo la classificazione della Strategia Nazionale di Cybersicurezza 2022-2026, vengono identificati "ordinari" e non "critici" o "strategici", sempre più spesso sono oggetto di attacchi ai propri sistemi informativi che causano grandi problemi alla gestione dell'attività amministrativa e all'erogazione dei servizi, fino a causarne il blocco per periodi prolungati.

In questo scenario, si inserisce il Decreto in esame, di recepimento della Direttiva (UE) 2022/2555 del Parlamento europeo che mira ad una omogeneizzazione delle misure di sicurezza cibernetica a livello degli Stati membri, riprendendo il percorso già tracciato con la Legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" recentemente emanata, che vuole indirizzare e sensibilizzare anche le Città Metropolitane, i Comuni con popolazione superiore a 100.000 abitanti, o comunque capoluogo di Regione, e loro in-house dedicate, in questo caso specifico in esame, alla gestione di servizi e sistemi informatici dedicati a settori individuati come altamente critici ai sensi degli Allegati I e II del decreto in esame.

Va detto infatti che, allo stato attuale, pur in presenza di casi virtuosi di singole amministrazioni comunali capaci di difendersi e rispondere agli attacchi in maniera efficace, per gli enti locali permane una generalizzata difficoltà ad attrezzarsi adeguatamente. I motivi principali che ostacolano l'adozione di adeguate misure di sicurezza, riassunti di seguito, non trovano, tuttavia, riscontro positivo nel testo in

esame, rimanendo irrisolti, a meno dell'adozione di misure di supporto successive o in fase di decretazione attuativa:

1. la carenza di risorse umane dipendenti con competenze tecniche adeguate, unita alla difficoltà a reperirne sul mercato di così specialistiche, anche a causa della bassa appetibilità, in termini retributivi, delle posizioni di lavoro all'interno dei Comuni;

2. la ristrettezza di risorse di bilancio da dedicare a interventi organizzativi e sui sistemi informativi;

3. l'impossibilità, quindi, di rispettare i dettami normativi e attuare le disposizioni previste ad invarianza finanziaria e di risorse umane, sia per le figure professionali richieste, sia per gli inevitabili adeguamenti informatici o rinnovi di licenze a nuove condizioni, necessari a rafforzare la resilienza cibernetica.

Commenti allo schema di decreto legislativo correttivo

In questa nota all'attenzione della IX Commissione della Camera dei Deputati si riportano le considerazioni e raccomandazioni che l'ANCI ha espresso in sede di Conferenza Unificata, ai fini del proprio parere, convocata per lo scorso 11 luglio.

Il decreto in esame recepisce la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, "relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2)" – che, conseguentemente, abroga a sua volta il d.lgs. 18 maggio 2018, n. 65, di recepimento della direttiva (UE) 2016/1148 (direttiva NIS).

Il decreto individua nell'Agenzia per la Cybersicurezza Nazionale -ACN- l'Autorità nazionale NIS responsabile dell'attuazione delle disposizioni del decreto in esame che opererà anche come Punto di contatto NIS nazionale nei confronti dell'UE, disciplinandone attività e responsabilità nei confronti dell'UE. La norma, inoltre, individua nella stessa Agenzia, con il ruolo di coordinatrice, affiancata dal Ministero della Difesa, l'Autorità di gestione delle crisi informatiche.

Il provvedimento è in linea con quanto previsto dalla Legge 28 giugno 2024, n. 90 recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", che per prima ha introdotto alcuni obblighi in capo, tra gli altri, alle città metropolitane, ai Comuni con popolazione superiore a 100.000 abitanti e, comunque, ai Comuni capoluoghi di regione, nonché alle loro società in-house, che gestiscono servizi e sistemi riferiti ad alcuni ambiti specifici, che, in questo caso si riferiscono a quelli ritenuti critici dagli Allegati I e II del testo in esame.

A tal proposito, le categorie di enti su menzionate, vengono ricomprese tra i soggetti importanti, come definiti dal decreto in esame, e fanno riferimento alla Presidenza del Consiglio dei Ministri quale Autorità di settore NIS.

Gli obblighi in capo ai soggetti importanti riguardano sia la comunicazione annuale di informazioni relative alla loro organizzazione in tema di gestione della cybersicurezza e ai servizi erogati, sia la notifica di minaccia o incidente informatico.

L'inadempienza agli obblighi può comportare sia l'applicazione di un regime sanzionatorio irrogato dall'ACN, sia l'applicazione della responsabilità disciplinare e dirigenziale nonché amministrativo-contabile, laddove, a seguito delle verifiche dell'ACN, l'ente non provveda ad attuare le indicazioni dell'Agenzia stessa, ovvero l'inadempienza venga reiterata nell'arco di cinque anni.

Tutto questo dovrà avvenire senza che derivino nuovi o maggiori oneri a carico della finanza pubblica, dovendo le Pubbliche Amministrazioni su menzionate provvedere

con le risorse umane, strumentali e finanziarie previste a legislazione vigente, ai sensi dell'art. 44 del decreto in esame.

Per quanto riportato in premessa in termini di ostacoli e difficoltà nell'adempiere alle nuove disposizioni in tema di Cybersicurezza per i Comuni, si riportano di seguito le raccomandazioni, già espresse, atte a favorire il potenziamento della resilienza cibernetica degli enti locali e l'attuazione concreta dei nuovi adempimenti, richiamando l'attenzione del Governo sulla necessità:

1. **di individuare le risorse necessarie all'applicazione della normativa in oggetto e le modalità di erogazione ai soggetti interessati, con particolare riguardo alle Pubbliche Amministrazioni locali, approfittando della disponibilità dei fondi PNRR in questa fase, ma delineando fin da ora un piano di investimenti che consenta la sostenibilità degli interventi anche successivamente**. Definire, quindi, un piano di finanziamenti nel medio-lungo periodo per supportare le Pubbliche amministrazioni locali nell'attuazione della norma e garantire la sostenibilità degli interventi nel tempo visto che, inevitabilmente, gli adempimenti non potranno essere a invarianza finanziaria dovendo gli enti attivare nuove procedure e sistemi che comportano la necessità di spese non previste e il reclutamento di personale specializzato;

2. **di coinvolgere maggiormente i Comuni e loro rappresentanze nella fase attuativa della normativa in esame e nella definizione degli atti regolamentari**, ed in particolare:
   - estendendo anche ai Comuni la partecipazione al Tavolo per l'attuazione della disciplina NIS, modificando l'art. 12 comma 2 inserendo un rappresentante aggiuntivo espressione dei Comuni, designato dalla Conferenza Unificata di cui al Dlgs 28 agosto 1997, n. 281, anziché della Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano;
   - coinvolgendo i Comuni, ricompresi nel perimetro di attuazione del presento decreto, nella fase di definizione degli atti attuativi e regolamentari, prevedendo un parere della Conferenza Unificata di cui al

Dlgs 28 agosto 1997, n. 281, laddove sia già previsto un confronto con gli enti territoriali.

3. di garantire il coordinamento e l'armonizzazione con le normative settoriali o, comunque, impattate dall'attuazione del presente decreto, in ottica di coerenza e semplificazione, al fine di facilitare la comprensione delle attività da svolgersi e ridurre le conseguenti sanzioni in caso di inadempienza, a carico dei soggetti individuati dalla norma in esame.