Camera – Resoconto Martedì 8 maggio 2018 pag. 36 Commissione speciale –

ALLEGATO 8

Schema di decreto legislativo recante attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Atto n. 10.

PARERE APPROVATO

La Commissione speciale per l'esame di atti del Governo, esaminato lo Schema di decreto legislativo di attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Atto n. 10);

ricordato che esso costituisce esercizio della delega attribuita dalla legge di delegazione europea 2016-2017 con riguardo alle direttive elencate in allegato, tra cui la direttiva (UE) 2016/1148 (inserita nell'Allegato A);

valutata positivamente la finalità di prevedere a livello europeo una disciplina uniforme concernente la sicurezza delle reti e dei sistemi informativi nazionali, nonché di incrementare il livello comune di sicurezza nell'Unione europea;

considerato che, da diversi anni, il tema della sicurezza cibernetica costituisce oggetto di analisi nell'ambito delle Relazioni sulla politica dell'informazione per la sicurezza trasmesse dalla Presidenza del Consiglio dei ministri al Parlamento, ai sensi dell'articolo 38 della legge n. 124 del 2007;

considerato altresì che nella relazione relativa all'anno 2017 si evidenzia la necessità di « rafforzare il presidio degli esercizi d'interesse, allo scopo di elevare gli standard di sicurezza nei prodotti hardware e software relativi al mercato unico digitale europeo e, allo stesso tempo, garantire agli asset strategici pubblici e privati del nostro Paese livelli di sicurezza adeguati alla minaccia »;

richiamate, al riguardo, le considerazioni ed i suggerimenti contenuti nel documento conclusivo dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico, svolta nella XVII legislatura dalla Commissione Difesa della Camera, approvato all'unanimità nella seduta del 21 dicembre 2017, nel quale si sottolinea la necessità di disporre e di sviluppare una specifica capacità ITC (Information and Communications Technology) in ambito nazionale nonché, in tale ottica, di sviluppare altresì la ricerca nel settore della sicurezza cibernetica all'interno di un più generale progetto strategico di sicurezza nazionale;

rilevato che lo schema di decreto in esame integra la vigente disciplina interna di rango legislativo e secondario che definisce l'architettura istituzionale deputata

alla tutela della sicurezza delle reti e prevede l'adozione di atti di indirizzo strategico (il « Quadro strategico nazionale 2013 ») e operativo (il « Piano nazionale cyber 2013 e 2017 ») attualmente in essere;

evidenziato come il decreto del Presidente del Consiglio del 17 febbraio 2017 – pur ripartendo la responsabilità della protezione dello spazio cibernetico nazionale tra più soggetti istituzionali in considerazione del carattere trasversale della minaccia – attuando il disposto dell'articolo 7-bis del decreto-legge n. 174 del 2015 assegni le funzioni di coordinamento e raccordo delle attività di prevenzione e gestione di eventuali situazioni di crisi di natura cibernetica alle strutture direttamente collegate al Comitato interministeriale per la sicurezza della Repubblica (CISR) e collochi, pertanto, il Nucleo per la sicurezza cibernetica (NSC) presso il Dipartimento Informazioni per la Sicurezza (DIS);

rilevato che il provvedimento in esame prevede l'adozione di una «strategia nazionale di sicurezza cibernetica » come atto di carattere generale recante obiettivi, priorità, governance del sistema, misure da adottare, programmi di formazione, piani di ricerca e sviluppo, valutazione dei rischi e indicazione dei soggetti coinvolti nella sua attuazione;

considerato che la direttiva (UE) 2016/1148 elenca all'allegato II i settori minimi per cui lo Stato membro deve mantenere un livello elevato di sicurezza delle reti e dei sistemi informativi, non escludendo però la possibilità di estendere tali settori in fase di recepimento;

considerato altresì che l'ambito di applicazione dello schema di decreto legislativo si concentra sul contenuto dell'allegato II (ossia energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali; nonché motori di ricerca, servizi cloud e piattaforme di commercio elettronico);

considerato inoltre che in ragione dell'imponente mole di dati (anche sensibili) e del ruolo chiave per l'economia e per la sicurezza del paese, appare opportuno effettuare una attenta valutazione dei settori della pubblica amministrazione da far rientrare nel campo di applicazione della normativa, utilizzando una valutazione il più possibile estensiva;

segnalato che la funzione di coordinamento nelle materie della sicurezza informatica ricoperta dal DIS risulta confermata ed estesa dal provvedimento in esame che individua proprio nel DIS il Punto di contatto unico;

evidenziato che la nuova disciplina trova applicazione sia nei confronti degli operatori di servizi essenziali, da inserire in un elenco nazionale redatto dalle autorità NIS, sia nei confronti dei fornitori di servizi digitali, che vengono, da un lato, chiamati ad adottare misure tecniche e organizzative relative alla gestione dei rischi, nonché alla prevenzione di incidenti e alla riduzione del loro impatto, dall'altro, assoggettati all'obbligo di notifica degli incidenti medesimi che abbiano un impatto rilevante sui servizi forniti;

osservato che l'articolo 8 del provvedimento in esame istituisce, presso la Presidenza del Consiglio dei ministri, un nuovo organismo, il CSIRT italiano – con un contingente di 30 unità di personale e lo stanziamento di specifiche risorse finanziarie – al quale sono attribuite le funzioni attualmente svolte dal CERT nazionale (Computer Emergency Response Team), presso il Ministero dello sviluppo economico, e dal CERT-PA, presso l'Agenzia per l'Italia digitale-AGID;
osservato altresì che tali funzioni sono attribuite al CSIRT italiano a decorrere dalla data di entrata in vigore di un decreto del Presidente del Consiglio dei ministri, che dovrà disciplinarne l'organizzazione e il funzionamento, di cui tuttavia non vengono precisati né i tempi di adozione né eventuali ulteriori elementi contenutistici;

rilevato che, nell'ambito dell'apparato sanzionatorio di cui all'articolo 21, la fattispecie oggetto di sanzione di cui al comma 2 non appare perfettamente corrispondente alla norma sostanziale ivi richiamata, di cui all'articolo 12, comma 2, giacché quest'ultima si riferisce puntualmente all'obbligo di adottare « misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza delle reti e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali »;

preso atto del parere favorevole espresso dalla Conferenza unificata in data 19 aprile 2018,

esprime

PARERE FAVOREVOLE

con le seguenti osservazioni:

a)
all'articolo 8, commi 2 e 9 – ove si affida ad un decreto del Presidente del Consiglio dei ministri l'organizzazione e il funzionamento del nuovo organismo che viene istituito (CSIRT italiano) a far data dall'entrata in vigore del medesimo decreto – si valuti l'opportunità di fissare i termini per l'adozione di tale atto ed eventualmente di precisarne ulteriormente i contenuti, al fine di evitare incertezze in sede applicativa anche alla luce degli obblighi recati dalla direttiva (UE) 2016/1148, oggetto di recepimento da parte dello schema di decreto in esame;

b)
si valuti l'opportunità di riformulare la fattispecie oggetto di sanzione di cui all'articolo 21, comma 2, conformemente a quanto previsto dall'articolo 12, comma 2, facendo riferimento alle « misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza delle reti e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali»;

c)

si valuti la possibilità di interpretare estensivamente l’ambito di applicazione della direttiva (UE) 2016/1148 comprendendovi, in particolare, anche la pubblica amministrazione.