COMMISSIONI RIUNITE

I (Affari costituzionali, della Presidenza del Consiglio e interni) e IX (Trasporti, poste e telecomunicazioni)

S O M M A R I O

ATTI DEL GOVERNO

Mercoledì 24 luglio 2024. — Presidenza del presidente della IX Commissione Salvatore DEIDDA.

La seduta comincia alle 9.05.

Schema di decreto legislativo recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.
Atto n. 164.

(Seguito dell'esame, ai sensi dell'articolo 143, comma 4, del Regolamento, e rinvio).

Le Commissioni proseguono l'esame dello schema di decreto all'ordine del giorno, rinviato nella seduta del 3 luglio 2024.

Salvatore DEIDDA, *presidente*, a seguito della richiesta di attivazione dell'impianto audiovisivo a circuito chiuso avanzata dal gruppo Partito Democratico, non essendovi obiezioni, ne dispone l'attivazione.

Avverte che è stato trasmesso il parere della Conferenza unificata.

Avverte altresì che si è concluso il ciclo di audizioni informali nell'ambito dell'esame del provvedimento e che sono pervenute memorie scritte, pubblicate, previo consenso, sul sito *internet* della Camera.

Enzo AMICH (FDI), *relatore per la IX Commissione,* anche a nome del relatore per la I Commissione Paolo Emilio Russo, formula una proposta di parere favorevole *(vedi allegato)*.

Ribadisce inoltre l'importanza del decreto legislativo in esame nella misura in cui dà attuazione ad una direttiva che appare oggi fondamentale, soprattutto alla luce dei recenti eventi che hanno interessato il settore dei trasporti, causati dai malfunzionamenti verificatisi in seno alla *CrowdStrike*.

Ringrazia gli uffici e il presidente per il lavoro svolto e per aver consentito di elaborare rapidamente una proposta di parere da portare all'attenzione delle altre forze politiche.

Illustra quindi la proposta di parere favorevole formulata.

Paolo Emilio RUSSO (FI-PPE), *relatore per la I Commissione,* intervenendo in videoconferenza, si associa alle considerazioni svolte dal collega Amich.

Matteo MAURI (PD-IDP), nel rilevare che la proposta illustrata dai relatori, pur esprimendo nelle premesse alcune possibili criticità, è una proposta di parere favorevole, fa presente che i parlamentari del Partito democratico hanno invece elaborato una serie di osservazioni al testo. In merito, chiede ai relatori se vi sia la disponibilità a integrare la proposta di parere testé illustrata, recependo alcune delle considerazioni dell'opposizione, preannunciando altrimenti la presentazione di una proposta alternativa di parere del gruppo del Partito democratico. A tal fine, chiede alla Presidenza quali siano i termini per la formulazione di tale proposta alternativa.

Salvatore DEIDDA, *presidente*, ricorda che una proposta alternativa di parere può essere presentata fino alla votazione della proposta di parere formulata dai relatori.

Enzo AMICH (FDI), *relatore per la IX Commissione,* manifesta la propria disponibilità a valutare le osservazioni elaborate dalle altre forze politiche, anche al fine di verificare se talune di queste siano già state contemplate all'interno della proposta di parere formulata.

Salvatore DEIDDA, *presidente*, nessun altro chiedendo di intervenire, rinvia il seguito dell'esame alla seduta già convocata per l'indomani.

La seduta termina alle 9.20.

ALLEGATO

Schema di decreto legislativo recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. Atto n. 164.

PROPOSTA DI PARERE

Le Commissioni riunite I (Affari Costituzionali) e IX (Trasporti),

esaminato lo schema di decreto legislativo recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;

svolto un ciclo di audizioni e acquisite le memorie di molti soggetti coinvolti nella disciplina sottoposta a parere;

preso atto del parere della Conferenza unificata;

preso atto che i destinatari delle disposizioni sono individuati secondo criteri molteplici e mediante categorie differenziate, adottando sia un criterio merceologico sia un limite dimensionale (cosiddetto *sizecap rule*). Più in particolare, l'articolo 3 del testo proposto individua – mediante il rinvio agli allegati I e II – settori altamente critici e critici; e – mediante il rinvio agli allegati III e IV – il novero delle amministrazioni pubbliche coinvolte. Inoltre, l'articolo 6, tra i soggetti inclusi nei diversi allegati, ne identifica due sottocategorie definite di soggetti essenziali e di soggetti importanti, ai fini di specifici obblighi da rispettare;

considerato che lo schema di decreto propone misure volte a garantire una maggiore sicurezza informatica in ambito nazionale, contribuendo a incrementare il livello comune di sicurezza nell'Unione europea, in modo da migliorare il funzionamento del mercato interno e rispondere al tempo stesso alle crescenti minacce derivanti dallo sviluppo dalla digitalizzazione;

visti gli articoli 8, comma 1, e 9, commi 1 e 2, della direttiva (UE) 2022/2555, secondo cui « *ogni Stato membro designa o istituisce una o più autorità competenti responsabili della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala (autorità di gestione delle crisi informatiche* » ed ha cura di indicare chiaramente quale di tali autorità deve fungere da coordinatore;

dal momento che l'articolo 2, comma 1, lettera *g)*, dello schema, definisce « *Autorità nazionali di gestione delle crisi informatiche* »: per la parte relativa alla resilienza nazionale di cui all'articolo 1 del decreto-legge n. 82 del 2021, l'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e, per la parte relativa alla difesa dello Stato, il Ministero della difesa, quali Autorità nazionali di gestione delle crisi informatiche di cui all'articolo 13, comma 1;

visto l'articolo 13, comma 1, dello schema, che individua l'Agenzia per la cybersicurezza nazionale, per la parte relativa alla resilienza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e il Ministero della difesa, per la parte relativa alla difesa dello Stato, quali Autorità nazionali di gestione delle crisi informatiche;

visti gli articoli 15, comma 2, e 89, comma 1, del decreto legislativo 15 marzo

2010, n. 66, Codice dell'ordinamento militare, che rispettivamente attribuiscono al Ministero della difesa, tra gli altri, la funzione e il compito di « *difesa e sicurezza dello Stato* » e alle Forze armate il « *compito prioritario di difesa dello Stato* »;

visto l'articolo 13, comma 3, dello schema, secondo cui, entro dodici mesi dalla data di entrata in vigore del decreto, con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale e del Ministero della difesa, ciascuno per gli ambiti di competenza, previo parere del Comitato interministeriale per la sicurezza della Repubblica nella composizione di cui all'articolo 10 del decreto-legge n. 82 del 2021, è definito il piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala;

considerato che la disciplina di cui al combinato disposto degli articoli 2, comma 1, lettera *g)*, e 13, comma 1, dello schema di decreto legislativo, risulta pienamente coerente con le competenze e le funzioni attribuite a ciascuna delle Autorità designate dalla normativa vigente e, alla luce della circostanza che gli incidenti e le crisi informatiche su vasta scala sono suscettibili di evolvere senza preavviso e con estrema immediatezza in un attacco alla sicurezza nazionale, garantiscono attraverso l'individuazione delle due Autorità l'immediato intervento negli ambiti di rispettiva competenza;

ritenuto auspicabile – con riguardo all'articolo 11 dello schema – che tutte le autorità di settore possano convergere su uno *standard* minimo comune e omogeneo di sicurezza;

ritenuto, con riguardo all'articolo 12 dello schema, che nella nozione di operatore privato invitato a partecipare al Tavolo per l'attuazione della disciplina NIS-2 possano rientrare anche le associazioni di categoria e di settore;

ritenuto che i costi in capo ai soggetti, inclusi nel perimetro di cibersicurezza e, comunque, destinatari degli obblighi previsti nello schema, saranno elevati e che, pertanto, si fa affidamento sulle autorità preposte che (ai sensi dell'allegato B alla legge di stabilità per il 2017 – n. 232 del 2016) i beni e i servizi dedicati alla cibersicurezza saranno considerati strumentali;

considerato che, nel futuro aggiornamento della disciplina della cibersicurezza, sarà necessario prevedere anche un sistema di *back-up* nazionale, anche per evitare i problemi verificatisi, per esempio, il 19 luglio 2024 nel settore dei trasporti, a causa del *crash* della CrowdStrike;

ritenuto, in merito all'articolo 25 relativo agli obblighi di notifica degli incidenti, in relazione ai quali è previsto il potere dell'ACN di adottare misure di semplificazione, che sarà necessario evitare duplicazioni nelle segnalazioni laddove le imprese, soggette al decreto legislativo, facciano parte dello stesso gruppo societario o siano al contempo fruitrici e fornitrici dei servizi per le infrastrutture critiche;

considerato, con riguardo all'articolo 27 relativo all'imposizione da parte dell'ACN alle imprese rientranti nell'ambito di applicazione del decreto legislativo di determinati prodotti, servizi e processi, che si tratta – in sintesi – dall'adozione di sistemi certificati. In tal senso, anche a mente dell'articolo 27, comma 2, l'ACN potrà rifarsi alle certificazioni sulla cibersicurezza già affermate a livello europeo (per esempio, l'ISO/IEC 27001 e ISO/IEC 22301);

ritenuto a proposito dell'articolo 28, relativo al potere dell'ACN di promuovere nei confronti dei soggetti rientranti nell'ambito di applicazione del decreto legislativo l'uso di specifiche tecniche e tecnologie per la mitigazione dei rischi, che l'esercizio di tale potere debba essere il più tempestivo possibile;

considerato che l'allegato IV dello schema fa riferimento anche ad « attività di ricerca » come oggetto sociale di soggetto cui incombono obblighi di cibersicurezza e che, quindi, sarà opportuno in sede applicativa specificare meglio che cosa s'intenda con tale nozione;

valutato che – con riguardo al tema della formazione del personale dei soggetti

destinatari delle disposizioni in via di emanazione – l'ACN svolge un ruolo importante in termini sia di supporto e guida sia di monitoraggio. In tale contesto, l'ACN potrà organizzare corsi appositi di formazione e di esercitazione sulla cibersicurezza. Inoltre, a mente del combinato disposto degli articoli 38 e 40 in materia di regime sanzionatorio, l'ACN potrebbe determinare la destinazione di una quota dei proventi delle sanzioni amministrative irrogate alle attività di formazione e ricerca sulla cibersicurezza;

considerato altresì, con riferimento all'articolo 37, la necessità che l'ACN tenga conto del profilo dimensionale degli operatori destinatari delle misure di esecuzione,

esprimono

PARERE FAVOREVOLE.