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

Giovedì 25 luglio 2024. — Presidenza del presidente della IX Commissione Salvatore DEIDDA. – Interviene la sottosegretaria di Stato per i rapporti con il Parlamento, Matilde Siracusano.

La seduta comincia alle 13.50.

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 conclusione – Parere favorevole).

Le Commissioni proseguono l'esame dello schema di decreto legislativo all'ordine del giorno, rinviato nella seduta del 24 luglio 2024.

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

Ricorda che i relatori, Paolo Emilio Russo per la I Commissione e Enzo Amich per la IX Commissione, hanno formulato nella seduta di ieri una proposta di parere *(vedi allegato 1)*.

Avverte che sono state presentate due proposte alternative di parere, rispettivamente, del Gruppo Azione *(vedi allegato 2)* e del Gruppo MoVimento 5 Stelle *(vedi allegato 3)*, che saranno poste in votazione solo qualora fosse respinta la proposta di parere dei relatori.

Enzo AMICH (FDI) ringrazia tutti i membri delle Commissioni I Affari costituzionali e IX Trasporti e i loro presidenti, per

lo svolgimento di un dibattito molto garbato e centrato sui contenuti.

Ringrazia inoltre anche il direttore generale dell'Agenzia per la cybersicurezza nazionale, Bruno Frattasi, per l'audizione ricca di spunti, nonché tutti i soggetti qualificati che hanno inviato memorie alle Commissioni.

Dichiara di aver consultato tutte le memorie ricevute dalle Commissioni e di averle trovate arricchenti. Osserva infatti che molti degli elementi in esse rinvenuti sono stati trasfusi nelle premesse del parere proposto alle Commissioni, d'intesa con il relatore per la I Commissione, il collega Russo.

Ribadisce l'importanza del testo esaminato, il quale investe questioni cruciali, come la cybersicurezza, la cyberdifesa, la tenuta complessiva dei sistemi di comunicazione e produzione nazionali.

Ricorda inoltre che la scorsa settimana, con il *crash* della *CrowdStrike* e la conseguente paralisi degli aeroporti, si è avuta ulteriore riprova di tale importanza.

Ringrazia anche i colleghi dell'opposizione, che correttamente hanno sollevato alcune questioni, quali, ad esempio, quella del *back up* nazionale, che appaiono meritevoli di attenzione e che certamente, in fase attuativa, il Governo e le autorità preposte terranno in considerazione.

Conferma poi, alla luce dell'interlocuzione, anche informale, con gli esponenti di maggioranza e con il Governo, la proposta di parere illustrato nella seduta di ieri, ritenendo che il testo dello schema realizzi un giusto equilibrio tra le varie istanze.

Per tali ragioni, non ritiene di formulare una proposta munita di condizioni o osservazioni, anche in considerazione del fatto che nelle premesse sono elencati molti degli spunti emersi nel corso della discussione.

Confida quindi che le amministrazioni interessate all'attuazione del decreto legislativo sapranno coglierne il senso ed orientarsi nella direzione di una piena valorizzazione dei contributi pervenuti, del rispetto dei diritti di cittadini, di famiglie e imprese, di una semplificazione degli adempimenti, e della protezione dell'integrità dei dati e dei sistemi informatici nazionali.

Andrea CASU (PD-IDP) presenta, a nome del gruppo del Partito Democratico, una proposta alternativa di parere *(vedi allegato 4)*, il cui contenuto risulta analogo al testo presentato dalla sua forza politica presso il Senato.

Si manifesta deluso per il comportamento tenuto dalle forze politiche di maggioranza, che con il parere presentato non hanno dato seguito all'ampio confronto portato avanti in questi mesi.

Ricorda, in particolare, i dati diffusi dall'Agenzia per la cybersicurezza nazionale, che vedono l'Italia al nono posto tra i Paesi vittima del maggior numero di attacchi informatici, con un aumento del 148 per cento rispetto agli anni precedenti.

A fronte di tali dati, critica l'azione del Governo, che reputa assolutamente non proporzionata alla gravità della situazione.

In particolare, afferma che la propria forza politica ha elaborato una serie di osservazioni delle quali auspica l'accoglimento all'interno del parere presentato dalla maggioranza. Ai fini dell'accoglimento, peraltro, non ritiene sufficiente una mera modifica delle premesse di suddetto parere, in quanto sostanzialmente prive di efficacia. Reputa al contrario necessaria la formulazione di una serie di osservazioni, in modo da ottenere una maggiore attenzione da parte del Governo.

Illustra poi i punti sui quali la proposta alternativa di parere presentata dalla propria forza politica si concentra, ricordando che si tratta di questioni emerse nel corso del dibattito parlamentare relativo ai provvedimenti precedentemente adottati sul tema.

Anzitutto, richiama l'importanza di adottare e dare effettiva attuazione ai criteri di adeguatezza e proporzionalità.

In secondo luogo, sottolinea l'importanza di valorizzare il ruolo del Parlamento attraverso la previsione di un parere parlamentare sui provvedimenti adottati in sede di attuazione della direttiva in materia di cybersicurezza. Ricorda inoltre che la necessità di un maggiore coinvolgimento delle Commissioni parlamentari sul tema è stata riconosciuta anche dal direttore generale dell'Agenzia per la cybersicurezza

nazionale, Bruno Frattasi, nel corso dell'audizione svolta.

Il terzo punto riguarda il tema delle risorse e, in particolare, la necessità di fornirle in misura adeguata alle imprese, in modo tale da mettere tali imprese effettivamente nelle condizioni di dare attuazione agli obblighi previsti dalla direttiva europea. Ricorda, nello specifico, che le risorse destinate alla cybersicurezza erano state originariamente contemplate nella misura dell'1,2 per cento degli investimenti nazionali. Tuttavia, tale previsione è stata ampiamente disattesa, in quanto soltanto lo 0,2 per cento degli investimenti nazionali è stato effettivamente destinato al settore.

Il quarto punto concerne la questione della legittima difesa e, nello specifico, la circostanza che gli operatori del settore, al fine di difendersi, sono costretti ad impiegare strumenti vietati dall'ordinamento giuridico. Ritiene pertanto necessario intervenire per evitare che chi agisce in adempimento degli obblighi imposti dalla direttiva europea e, quindi, dal presente provvedimento non incorrano nelle pene previste dall'articolo 635-*quater* del Codice penale.

Il quinto punto riguarda il coinvolgimento dei comuni non capoluoghi di regione o con meno di 100.000 abitanti. Sul punto, ritiene opportuno adottare un criterio che non sia meramente matematico, ma che tenga invece conto delle reali esigenze del territorio.

Rileva poi la necessità di introdurre un obbligo di relazione periodico in ambito di cybersicurezza e la predisposizione di un tavolo di confronto che coinvolga anche il settore dell'industria.

Infine, l'ultimo tema concerne la previsione di norme per la sicurezza della *supply chain* attraverso incentivi al mercato unico europeo. Ricorda infatti quanto il sistema europeo di cybersicurezza appaia fragile e necessiti di maggiori interventi da parte degli Stati membri. Reputa inoltre necessario implementare una politica industriale ed economica che renda l'Italia e l'Unione europea protagoniste a livello mondiale, anziché dipendenti dalle economie degli altri Paesi.

In conclusione, chiede l'accoglimento di tali punti attraverso la formulazione di specifiche osservazioni o condizioni all'interno del parere della maggioranza, reputandole necessarie anche alla luce di quanto accaduto durante l'esame del provvedimento presso il Senato, dove molte delle condizioni ed osservazioni inizialmente formulate sono state poi eliminate.

Conclude infine annunciando l'astensione della propria forza politica nella votazione della proposta di parere formulata dai relatori, nell'eventualità in cui tali richieste non venissero accolte. Infatti, pur accogliendo con favore il recepimento della direttiva NIS-2, ribadisce di non condividere la scelta dei relatori di formulare una proposta di parere priva di condizioni e osservazioni.

Antonino IARIA (M5S) illustra la proposta alternativa di parere favorevole con condizioni, presentata dal MoVimento 5 Stelle. A suo giudizio il Governo non comprende come la scelta di non investire in cybersicurezza crei un gravissimo pericolo per l'economia reale del Paese e specialmente per le piccole e medie imprese italiane, che hanno ad oggi uno scarsissimo livello di protezione. Sottolinea inoltre il rischio che dagli attacchi *hacker* possano derivare ingenti proventi illeciti a vantaggio della criminalità organizzata e di quegli intermediari che contribuiscono ad alimentare un mercato parallelo e contiguo alla criminalità stessa.

Sostiene che il Parlamento avrebbe potuto fare di più con il disegno di legge « cybersicurezza » e potrebbe essere più attivo anche rispetto al recepimento delle norme del diritto dell'Unione europea. Fa presente che nella proposta di parere alternativa è stato ripreso il contenuto di emendamenti presentati al citato disegno di legge e, tra le condizioni poste, richiama quelle concernenti la necessità di un monitoraggio parlamentare sull'azione del Governo, la destinazione dei proventi delle sanzioni ad interventi di reinvestimento in cybersicurezza, l'estensione del tavolo per l'attuazione della disciplina NIS a rappresentanti delle autonomie locali, nonché il conferimento di risorse per il supporto e

l'accompagnamento dei soggetti interessati dal provvedimento in esame.

Ritenendo poi che il recente grave *bug* non possa essere sminuito, considerata la sua portata, sottolinea che solo con una reale consapevolezza dei pericoli effettivi non saranno sottovalutati in futuro questi attacchi. Qualora invece manchino programmazione e investimenti nell'istruzione – a tutti i livelli – si lavorerà sempre e solo sui danni e mai su un'efficace prevenzione.

Preannuncia dunque l'astensione del MoVimento 5 Stelle nella votazione della proposta di parere formulata dai relatori. Pur dichiarandosi infatti favorevole al recepimento della direttiva NIS-2, non condivide le scelte del Governo, che non potrà ottenere risultati positivi senza destinare risorse per l'istruzione sul tema della cybersicurezza, senza investimenti in ricerca e sviluppo e senza incentivi per i soggetti privati coinvolti dal provvedimento in esame.

La sottosegretaria Matilde SIRACUSANO esprime un orientamento positivo sulla proposta di parere favorevole dei relatori.

Nessun altro chiedendo di intervenire, le Commissioni approvano la proposta di parere favorevole dei relatori *(vedi allegato 1)*.

Salvatore DEIDDA, *presidente*, dichiara che a seguito dell'approvazione della proposta di parere dei relatori risulta preclusa la votazione delle proposte alternative di parere dei Gruppi Azione, MoVimento 5 Stelle e Partito Democratico.

La seduta termina alle 14.10.

ALLEGATO 1

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.

PARERE APPROVATO

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 (c.d. *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 (ACN), 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, recante 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.

ALLEGATO 2

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 ALTERNATIVA DI PARERE DEL GRUPPO AZ-PER-RE

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 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;

tenuto conto di quanto previsto dall'articolo 2, comma 7 e 8, della direttiva (UE) 2022/2555, i criteri di individuazione dei soggetti esenti dall'applicazione della normativa di cui all'articolo 4, comma 4, risulta tuttavia eccessivamente vaga e rischia di coinvolgere un numero di soggetti esteso tanto da porre potenzialmente in essere dei rischi per gli interessi nazionali e commerciali;

considerato, con riguardo all'articolo 27, concernente l'imposizione da parte dell'ACN (Agenzia per la Cybersicurezza Nazionale) 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 in considerazione del disposto dello stesso articolo 27, comma 2, si ritiene necessario che l'ACN si rifaccia alle certificazioni e agli *standard* tecnici sulla cibersicurezza già affermate a livello internazionale (per esempio, l'ISO/IEC 27001 e ISO/IEC 22301);

ritenuto opportuno che, riguardo all'applicazione dell'articolo 28, comma 1, si ponga una particolare e maggiore attenzione all'integrazione della normativa nazionale con le direttive europee e le altre normative settoriali esistenti, grazie anche ad un impegno attivo di ACN;

considerato che l'articolo 16, comma 3, prevede la possibilità per persone fisiche o giuridiche di segnalare una vulnerabilità al CSIRT Italia (*Computer Security Incident Response Team – Italia*), in sede di applicazione del suddetto articolo appare necessario garantire tutele solide e concrete ai suddetti segnalatori che vadano oltre la semplice garanzia di anonimato, al fine di evitare che la collaborazione dei segnalatori venga inibita dal timore di conseguenze negative,

esprimono

PARERE FAVOREVOLE

con le seguenti osservazioni:

valuti il Governo l'opportunità di:

1) in sede applicativa, chiarire e delineare in maniera più precisa la defini-

zione dei soggetti esentati di cui all'articolo 4, comma 4;

2) prevedere delle forme di tutela solide e garantite, aggiuntive al mero anonimato, nei confronti dei segnalatori di vulnerabilità di cui all'articolo 16, comma 3;

3) applicare le misure necessarie affinché l'Agenzia per la cybersicurezza nazionale: promuova e favorisca attivamente l'applicazione di norme settoriali quanto più armonizzate all'interno dello stesso settore per quanto riguarda le tipologie di soggetti di cui agli allegati I, II, III e IV del presente decreto al fine di evitare sovrapposizioni ed inefficienze e di assicurare una maggiore conformità e sicurezza; consulti i documenti di consulenza e orientamento riguardanti i settori tecnici e le norme già esistenti, comprese le norme nazionali, che potrebbero essere applicate a tali settori elaborati da ENISA come da articolo 25 paragrafo 2 della direttiva (UE) 2022/2555; collabori alla stesura dei documenti stessi ed elabori documenti propri di indirizzo.

Pastorella.

ALLEGATO 3

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 ALTERNATIVA DI PARERE DEL GRUPPO M5S

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

esaminato l'atto del Governo in titolo,

premesso che:

l'atto in titolo attua il recepimento della direttiva europea cosiddetta « NIS-2 » che reca la legislazione dell'Unione europea in materia di cibersicurezza e prevede misure giuridiche per rafforzare il livello generale di cibersicurezza nell'Unione;

le norme dell'Unione europea in materia di cibersicurezza introdotte nel 2016 sono state aggiornate dalla direttiva NIS-2, entrata in vigore nel 2023, con la quale è stato modernizzato il quadro giuridico esistente per tenere il passo con una maggiore digitalizzazione e un panorama in evoluzione delle minacce alla cibersicurezza, estendendo l'ambito di applicazione delle norme in materia di cibersicurezza a nuovi settori e entità, migliorando ulteriormente la resilienza e le capacità di risposta agli incidenti degli enti pubblici e privati, delle autorità competenti e dell'Unione nel suo complesso;

la direttiva NIS-2, sulle misure per un livello comune elevato di cibersicurezza in tutta l'Unione, è volta a:

garantire la preparazione degli Stati membri, imponendo loro di essere adeguatamente equipaggiati. Ad esempio, con un *team* di risposta agli incidenti di sicurezza informatica (CSIRT) e un'autorità nazionale competente in materia di reti e sistemi informativi (NIS); la cooperazione tra tutti gli Stati membri, istituendo un « gruppo di cooperazione » per sostenere e facilitare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri; una cultura della sicurezza in tutti i settori che sono vitali per la nostra economia e società e che dipendono fortemente dalle TIC, come l'energia, i trasporti, l'acqua, le infrastrutture bancarie, dei mercati finanziari, l'assistenza sanitaria e le infrastrutture digitali;

prevedere, per le imprese identificate dagli Stati membri come operatori di servizi essenziali nei settori summenzionati, l'adozione di misure di sicurezza adeguate e la notifica alle autorità nazionali competenti gli incidenti gravi e per i principali fornitori di servizi digitali, quali i motori di ricerca, i servizi di *cloud computing* e i mercati *online*, il rispetto di specifici obblighi di sicurezza e notifica;

il provvedimento è da ritenersi complementare e funzionale alla legge approvata di recente dalle Camere – legge 28 giugno 2024, n. 90 – che ha anticipato l'attuazione di talune disposizioni e tematiche recate dalla direttiva europea NIS-2, in ordine al quale i firmatari avevano segnalato carenze e omissioni cui si sarebbe potuto porre rimedio nell'occasione in parola e che invece riverberano anche nell'atto del Governo in esame, cui si aggiungono ulteriori profili critici, come di seguito evidenziato;

nel complesso, si rileva:

un rinvio massiccio a non meglio precisate « determinazioni » dell'Agenzia per la cybersicurezza nazionale e a decreti del Presidente del Consiglio – quest'ultimo, in particolare, strumento normativo atipico

da considerarsi atto di natura politica che, nei numerosissimi casi di cui all'atto in titolo, oltre alla previsione di poter essere adottato in deroga all'articolo 17 della legge ordinamentale 23 agosto 1988, n. 400, intacca il sistema di produzione delle fonti normative ed elude ruolo, potestà e prerogative parlamentari, comprese le funzioni in termini di indirizzo e controllo;

la necessità del parere del Comitato parlamentare per la sicurezza della Repubblica in ordine alle disposizioni di cui all'articolo 4, commi 4 e 5 – concernenti, rispettivamente, l'individuazione dei soggetti che svolgono attività o forniscono servizi in via esclusiva per gli enti, organi e articolazioni della pubblica amministrazione di cui al comma 3, nonché in materia di protezione civile e « i soggetti che svolgono attività o forniscono servizi in via esclusiva per gli Organismi di informazione per la sicurezza nazionale » – all'articolo 9, comma 4 – concernente la valutazione periodica della Strategia nazionale di cybersicurezza – all'articolo 14, comma 2, lettera *d)* – concernente l'elenco dei soggetti che impattano sull'efficienza dello strumento militare e sulla tutela della difesa e sicurezza militare dello Stato, su cui l'Autorità nazionale competente NIS comunica tempestivamente al Ministero della difesa gli incidenti nonché le ulteriori informazioni di sicurezza cibernetica;

l'opportunità del coinvolgimento preventivo e delle valutazioni del Garante per la protezione dei dati personali in ordine alle disposizioni di cui all'articolo 4, commi 7 e 8 – concernenti, rispettivamente, l'apodittica esclusione, nell'ambito degli obblighi informativi stabiliti nell'atto in titolo di informazioni la cui divulgazione sia contraria agli interessi essenziali dello Stato italiano in materia di sicurezza nazionale, pubblica sicurezza o difesa e lo scambio delle informazioni riservate, rilevanti anche in campo degli interessi commerciali dei soggetti essenziali e importanti – all'articolo 8, concernenti (anche) il trattamento dei dati personali da parte dei fornitori di reti pubbliche di comunicazione elettronica o dei fornitori di servizi di comunicazione elettronica accessibili al pubblico, nonché all'articolo 14 – concernente la cooperazione e gli scambi tra Autorità nazionali, in cui l'apporto del Garante appare limitato successivamente a casi di violazioni gravi e specifiche; il predetto coinvolgimento e le predette valutazioni del Garante *privacy* dovrebbero essere assunti in ordine al contenuto dei DPCM e delle determinazioni dell'Agenzia di cui al presente atto ove essi concernono oggetti e temi di competenza;

l'assenza delle autonomie locali, pur pienamente coinvolte nell'attuazione della direttiva e dei relativi obblighi e procedure, anche con riguardo alle loro società *in house*, dal Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 e, al contrario, in ordine al medesimo articolo, al comma 3, la non meglio precisata presenza, al medesimo Tavolo, di « operatori privati interessati dalle previsioni di cui al presente decreto »;

gli obblighi in materia di gestione, prevenzione e riduzione dei rischi per la sicurezza informatica di cui al presente atto si aggiungono a quelli recati dalla predetta legge n. 90 del 2024 e, parimenti, comportano l'adozione di misure tecniche, operative e organizzative specifiche ed adeguate che risultano essere a carico dei soggetti obbligati, in assenza di risorse finanziarie o incentivi, di azioni di sostegno o di accompagnamento, anche da parte dell'Agenzia – non è da ritenersi sufficiente il supporto offerto ai sensi delle disposizioni di cui all'articolo 35, comma 2, supporto limitato, peraltro, ai sensi del comma 6, espressamente ai casi in cui il supporto medesimo « non costituisca un onere sproporzionato o eccessivo »; in proposito, risulterebbe opportuno l'obbligo per l'Agenzia, in luogo della mera facoltà di cui all'articolo 37, comma 5, di designare un proprio funzionario – sembrerebbe necessario, in vero, un vero e proprio *pool* di funzionari, una sorta di *task force* – da destinare al supporto dei soggetti pubblici e ad incentivi per i soggetti privati obbligati agli adempimenti; in proposito, si reputa necessario prevedere un sostegno finanziario sistematico ai fini del rafforzamento della cybersicurezza nazionale, prevedendo

che i proventi delle sanzioni disposte nei casi di reiterata inosservanza dell'obbligo di notifica degli incidenti di sicurezza informatica e degli attacchi informatici siano destinati, in parte, all'incremento del Fondo per l'innovazione, come già previsto dall'articolo 18-*bis* del Codice dell'amministrazione digitale, ai fini del sostegno, in particolare, del potenziamento della capacità di resilienza delle autonomie locali;

la perplessità in ordine all'applicazione della causa di responsabilità contabile ai dipendenti pubblici che agiscono in violazione dei relativi obblighi disposti dall'atto in titolo nell'esercizio delle loro funzioni, a fronte della perdurante esclusione della predetta responsabilità, stante la vigenza del cosiddetto « scudo contabile », attualmente, e in assenza di un eventuale ulteriore proroga, in vigore fino al 31 dicembre 2024;

si ribadiscono, in questa sede, le criticità rilevate in sede d'esame del disegno di legge in materia di cybersicurezza – ora legge n. 90/2024 – in ordine a:

la necessità di prevedere un obbligo per l'Agenzia, in luogo della mera facoltà disposta dalla legge n. 90/2024, di individuare modalità e processi di coordinamento e di mutua collaborazione, anche di livello regionale, tra le amministrazioni e tra i referenti per la cybersicurezza al fine di facilitare la resilienza delle amministrazioni pubbliche;

la posizione indeterminata e priva di specifici requisiti, qualifiche e competenze del referente per la cybersicurezza, che risulta differenziato rispetto ai responsabili per la transizione digitale e per la protezione dei dati nelle pubbliche amministrazioni e la mancata previsione di corsi di formazione iniziali e periodici, questioni che si reputano necessarie e imprescindibili, stante la necessità di un alto livello di cybersicurezza a fronte dell'incremento e della natura in continua evoluzione delle minacce e dei rischi informatici e dell'evoluzione della tecnologia;

la necessità dell'adozione di un regolamento, con la supervisione del Ministero della giustizia e dell'interno e il coinvolgimento dell'Agenzia, finalizzato a garantire *standard* uniformi di sicurezza nei dispositivi e nelle tecnologie degli uffici giudiziari;

l'assenza di misure e di risorse ai fini della promozione e della realizzazione, da parte dell'Agenzia, d'intesa con il Ministro dell'istruzione e del merito, di corsi specifici al fine di favorire in tutti i livelli del sistema educativo una progressiva familiarizzazione degli studenti con la sicurezza informatica nonché l'assenza di iniziative per favorire la diffusione della cultura della sicurezza informatica tra i cittadini, con particolare riguardo alle categorie a rischio di esclusione, con azioni specifiche e concrete, anche avvalendosi di un insieme di strumenti e mezzi diversi, fra i quali il servizio radiotelevisivo, e del coinvolgimento di università, centri di ricerca e di formazione specializzati;

considerato che:

l'assenza di congrue risorse finanziarie mette a rischio l'attuazione dell'atto in titolo e della legge n. 90 del 2024, si pone in aperta contraddizione con i pur lodevoli intenti dichiaratamente perseguiti, i quali necessiterebbero, oltre a quanto rilevato, di un piano di investimenti in ricerca e sviluppo nel settore della sicurezza informatica unitamente ad un solido e funzionale incremento di indirizzi accademici e professionali per formare figure specializzate in strategie e tecnologie di sicurezza informatica;

la predetta assenza e il complesso dei nodi critici sopra rilevati riducono la possibilità, per l'atto in titolo, di soddisfare i propositi e di adempiere agli obiettivi della direttiva NIS-2, né paiono in grado di aumentare la capacità di resilienza e risposta delle pubbliche amministrazioni e degli altri soggetti ivi obbligati,

esprimono

PARERE FAVOREVOLE

con le seguenti condizioni:

1) siano previsti il parere delle Commissioni parlamentari competenti per ma-

teria e per i profili finanziari preliminarmente all'adozione dei decreti del Presidente del Consiglio di cui al testo dell'atto in titolo e delle determinazioni dell'Agenzia per la cybersicurezza nazionale nonché il coinvolgimento del Comitato parlamentare per la sicurezza della Repubblica e del Garante per la protezione dei dati personali in ordine a quanto indicato, rispettivamente, ai punti n. 1, 2 e 3 di cui alla premessa;

2) sia previsto che i proventi delle sanzioni disposte nei casi di reiterata inosservanza dell'obbligo di notifica degli incidenti di sicurezza informatica e degli attacchi informatici siano in parte destinati all'incremento del Fondo per l'innovazione ai fini del sostegno, in particolare, del potenziamento della capacità di resilienza delle autonomie locali;

3) sia esteso alla partecipazione di rappresentanti delle autonomie locali il Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 e, in attuazione del principio di trasparenza, siano resi noti gli inviti al Tavolo medesimo ove estesi agli « operatori privati interessati »;

4) siano previste misure costanti di supporto e accompagnamento, ai fini dell'implementazione della resilienza cibernetica ed informatica, da parte dell'Agenzia a favore dei soggetti pubblici obbligati ai sensi dell'atto in titolo e della legge n. 90 del 2024;

5) siano adottate congrue misure finanziarie da destinare al sostegno rispetto all'adempimento degli obblighi in materia di gestione, prevenzione e riduzione dei rischi per la sicurezza informatica da parte dei soggetti pubblici di cui al presente atto e alla predetta legge n. 90 del 2024 nonché ad incentivi per i soggetti privati parimenti obbligati di minori dimensioni;

6) siano previsti corsi di formazione iniziali e periodici per i referenti per la cybersicurezza, stante la necessità di un alto livello di cybersicurezza a fronte dell'incremento e della natura in continua evoluzione delle minacce e dei rischi informatici e dell'evoluzione della tecnologia;

7) siano previsti corsi specifici al fine di favorire in tutti i livelli del sistema scolastico, e ad essi adeguati, una progressiva familiarizzazione degli studenti con la sicurezza informatica nonché iniziative per favorire la diffusione della cultura della sicurezza informatica tra i cittadini;

8) siano assunte le misure necessarie all'adozione di un regolamento finalizzato a garantire *standard* uniformi di sicurezza nei dispositivi e nelle tecnologie degli uffici giudiziari;

9) provveda il Governo a prevedere ed illustrare alle Camere un piano di investimenti in ricerca e sviluppo nel settore della sicurezza informatica unitamente ad un programma recante un solido e funzionale incremento di indirizzi accademici e professionali per formare figure specializzate in strategie e tecnologie di sicurezza informatica.

Alfonso Colucci, Iaria, Alifano, Auriemma, Penza, Cantone, Fede, Traversi.

ALLEGATO 4

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 ALTERNATIVA DI PARERE DEL GRUPPO PD-IDP

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

esaminato lo schema di decreto legislativo di recepimento della direttiva (UE) 2022/2555, 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 (A.G. 164);

premesso che:

con la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio (cosiddetta direttiva NIS) il legislatore europeo ha posto le basi per sviluppare le capacità di cybersicurezza in tutta l'Unione al fine di mitigare le minacce ai sistemi informativi e di rete utilizzati per fornire servizi essenziali in settori chiave e garantire la continuità di tali servizi in caso di incidenti, contribuendo in tal modo alla sicurezza dell'Unione e al funzionamento efficace della sua economia e della sua società;

la direttiva NIS ha garantito il completamento dei quadri nazionali, definendo le rispettive strategie sulla sicurezza dei sistemi informativi e di rete, stabilendo capacità nazionali, nonché attuando misure normative riguardanti le infrastrutture e gli attori essenziali individuati da ciascuno Stato membro. Inoltre, ha contribuito alla cooperazione a livello dell'Unione mediante l'istituzione del gruppo di cooperazione e della rete di gruppi nazionali di intervento per la sicurezza informatica in caso di incidente;

nonostante tali risultati, l'applicazione della direttiva NIS ha rivelato, alla luce della rapida evoluzione della tecnologia, una serie di carenze intrinseche che allo stato attuale limitano la capacità di affrontare efficacemente le sfide attuali ed emergenti in materia di cybersicurezza;

con la direttiva (UE) 2022/2555 (cosiddetta direttiva NIS-2) del Parlamento europeo e del Consiglio del 14 dicembre 2022, viene abrogata la direttiva NIS e vengono poste in essere misure per superare tali carenze;

il nuovo impianto posto in essere dalla direttiva NIS-2 mira pertanto a superare e rafforzare quanto già previsto dalla precedente direttiva NIS, recepita nell'ordinamento nazionale con il decreto legislativo 18 maggio 2018, n. 65 (decreto legislativo « NIS »), in particolare attraverso: l'ampliamento del campo di applicazione, includendo anche la pubblica amministrazione centrale, le piccole e microimprese nel caso in cui operino in settori chiave per la società e, indipendentemente dalle dimensioni, fornitori di servizi di comunicazione elettroniche pubbliche e di reti di comunicazione elettronica accessibili al pubblico, con un aumento significativo dei settori vigilati e l'introduzione di un approccio « *allhazards* » alla cybersicurezza, che prevede l'inclusione di profili di sicurezza fisica delle infrastrutture ICT (*Information and Communications Technology*); la revisione del meccanismo di identificazione dei soggetti quali entità importati o essenziali, prevedendo un criterio omogeneo basato sulla dimensione (cosiddetto *sizecap rule*), che estende l'applicazione della direttiva a tutte le medie e grandi imprese che operano nei settori iden-

tificati, ciò al fine di superare l'attuale disomogeneità nel processo di identificazione dei soggetti da parte degli Stati membri; il rafforzamento dei poteri di supervisione, con indicazioni più dettagliate per la definizione delle misure di sicurezza e l'inasprimento delle sanzioni; l'ampliamento delle funzioni dei CSIRT (*Computer Security Incident Response Team*) nazionali, che fungeranno, tra l'altro, da intermediari di fiducia tra i soggetti segnalanti e i fornitori di prodotti e servizi ICT nell'ambito del quadro per la divulgazione coordinata delle vulnerabilità (*Coordinated Vulnerability Disclosure* ± CVD); la gestione delle crisi, con la previsione di una strategia in materia e l'istituzionalizzazione della *Cyber Crises Liaison Organisation Neiwork* (CyCLONe), per la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala;

considerato che:

nel corso degli ultimi anni, a livello nazionale, anche in ragione del contesto geopolitico, influenzato dai conflitti in Ucraina e in Medio Oriente, si è registrato un consistente aumento di azioni *cyber* malevoli, principalmente eventi di tipo DDoS a danno di siti *web* di pubbliche amministrazioni e imprese e, in numero esiguo, di tipo *defacement*, ossia intrusioni informatiche che consistono nel modificare pagine di siti *web* sostituendole con un messaggio di rivendicazione, di apologia e simili;

un'altra minaccia in aumento è costituita dagli attacchi *ransomware*, ossia, operazioni tramite le quali l'attaccante, di regola, si introduce nei sistemi di un soggetto per cifrarne i dati, al fine di ottenere il pagamento di un riscatto necessario a rendere le informazioni nuovamente disponibili al legittimo proprietario e/o a non diffonderle pubblicamente;

nel contesto nazionale sopra illustrato, dunque, l'attuazione della direttiva NIS-2 appare indispensabile per promuovere l'utilizzo di reti e sistemi sicuri, specialmente quando funzionali all'operatività delle infrastrutture cruciali per la tenuta del Sistema Paese, e mitigare le criticità che, come richiamato, sono state rilevate anche in ambito nazionale, con particolare riguardo alla ristrettezza dell'ambito di applicazione e all'ambiguità sulla individuazione dei soggetti cui rivolgere le misure di sicurezza e gli obblighi previsti dalla direttiva NIS;

l'Agenzia per la cybersicurezza nazionale, istituita con il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni dalla legge 4 agosto 2021, n. 109, con il compito tutelare la sicurezza e la resilienza nello spazio cibernetico, ha rafforzato il proprio impegno per garantire la diffusione di informazioni sui rischi *cyber* oltre che per fornire assistenza alle vittime. Tuttavia occorrono nuovi strumenti per affrontare le crescenti problematiche di sicurezza a fronte della continua evoluzione tecnologica;

rilevato che:

nella redazione dello schema di decreto legislativo di recepimento, nel tenere conto dei criteri e dei principi direttivi di delega, contenuti nell'articolo 3 della legge 21 febbraio 2024, n. 15 (delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea legge di delegazione europea 2022-2023), gran parte dei contenuti della direttiva NIS-2 sono stati recepiti ma emergono, comunque, alcune importanti lacune meritevoli di maggiore attenzione anche alla luce degli effetti dei recenti accadimenti verificatasi lo scorso 19 luglio 2024, che hanno portato al *crash* dei sistemi informatici a livello internazionale,

esprimono

PARERE FAVOREVOLE

con le seguenti osservazioni:

1) sia previsto che l'attuazione e l'implementazione della normativa si basi su dettagliati criteri di adeguatezza e proporzionalità delle misure di sicurezza, sia in funzione del livello di rischio analizzato, sia rispetto all'esposizione e tipologia del soggetto identificato (differenziando, quindi, tra soggetti importanti ed essenziali), sia

rispetto alla valutazione di impatto sui sistemi informativi e di rete;

2) relativamente ai provvedimenti di normazione secondaria di attuazione della direttiva NIS-2 che spettano all'ACN, sia prevista la trasmissione al Parlamento per l'espressione di un parere, in modo da avere un confronto costante tra legislatore e ACN stessa;

3) relativamente all'articolo 9, che richiama la Strategia Nazionale per la Cibersicurezza come strumento per individuare obiettivi e risorse strategiche nell'ambito degli adempimenti comunitari, siano previste adeguate misure che consentano di raggiungere l'obiettivo del 1,2 per cento degli investimenti nazionali per la cibersicurezza già previsto dalla suddetta Strategia Nazionale, al momento disatteso;

4) sia chiarita l'interpretazione esatta dell'articolo 635-*quater* comma 1 del Codice penale, come modificato dalla legge 90 del 2024 che punisce l'utilizzo « abusivo » di una serie di attività *cyber*, definendo il significato preciso del termine « abusivo » sopra ricordato, in particolare stabilendo che tutti i privati che svolgono attività volte all'adempimento della direttiva in oggetto, così come i loro fornitori quando agiscono sempre per adempiere alla NIS-2, agiscono legittimamente e non rientrano nella fattispecie del citato articolo 635-*quater*, comma 1, Codice penale sopra ricordato;

5) si valuti di poter ricomprendere nella normativa anche i comuni non capoluoghi di regione o inferiori ai 100.000 abitanti, su indicazione dell'ACN;

6) sia previsto per le società private coinvolte nell'applicazione della normativa un obbligo di *reporting* periodico in ambito *cybersecurity* al *board*, se presente, per finalità di monitoraggio e indirizzo delle priorità strategiche di settore;

7) sia prevista all'articolo 12, anche in apposita sessione all'uopo istituita, la partecipazione dell'industria al Tavolo per l'attuazione della direttiva NIS, attraverso il coinvolgimento delle associazioni di categoria e delle società private maggiormente rappresentative dei vari settori;

8) siano previste norme per la sicurezza della *supply chain* attraverso incentivi al mercato unico europeo dei prodotti di sicurezza.

Mauri, Casu, Bonafè, Barbagallo, Bakkali, Cuperlo, Fornaro, Ghio, Morassut.