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

La seduta comincia alle 13.30.

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.

(Esame, ai sensi dell'articolo 143, comma 4, del regolamento, e rinvio).

Le Commissioni iniziano l'esame dello schema di decreto all'ordine del giorno.

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 la richiesta di parere parlamentare sull'atto in esame non è corredata dal previsto parere della Conferenza unificata. Le Commissioni non potranno dunque pronunciarsi definitivamente sull'atto prima che il Governo abbia provveduto ad integrare la richiesta di parere in tal senso.

Paolo Emilio RUSSO (FI-PPE), *relatore per la I Commissione*, fa presente che le Commissioni riunite Affari costituzionali e Trasporti sono chiamate a esaminare, ai fini dell'espressione del parere al Governo, lo schema di decreto legislativo Atto Governo n. 164, di 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. Rammenta che attraverso lo schema il Governo dà attuazione alla delega conferitagli dagli articoli 1 e 3 della legge di delegazione europea 2022-2023 (legge n. 15 del 2024), che individuano specifici principi e criteri di delega per il recepimento della direttiva (UE) 2022/2555 del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione europea, c.d. « direttiva NIS 2 », che deve essere attuata entro il 17 ottobre 2024.

Prima di affrontare il contenuto dell'articolato, ritiene essenziale inquadrare la c.d. Direttiva NIS 2 nell'ambito della tutela della sicurezza cibernetica nell'Unione europea, ricordando che la materia è stata inizialmente regolata dalla direttiva (UE) 2016/1148 del 6 luglio 2016 che reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. direttiva NIS – *Network and Information Security*) al fine di conseguire un « livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea ». La direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 18 maggio 2018 (c.d. decreto legislativo NIS), che detta la cornice legislativa interna delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS. Sottolinea che le norme europee introdotte nel 2016 sono state aggiornate dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 (c.d. direttiva NIS 2) che sostituisce il quadro di riferimento in materia, al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cibersicurezza. L'aggiornamento della direttiva mira inoltre ad eliminare le ampie divergenze tra gli Stati membri che hanno attuato gli obblighi in materia di sicurezza e segnalazione degli incidenti, nonché in materia di vigilanza ed esecuzione, stabiliti dalla direttiva NIS in modi significativamente diversi a livello nazionale, con un effetto potenzialmente pregiudizievole sul funzionamento del mercato interno. In particolare, la direttiva NIS 2 stabilisce norme minime e meccanismi per la cooperazione tra le autorità competenti di ciascuno Stato membro, aggiornando l'elenco dei settori e delle attività soggetti agli obblighi in materia di cybersicurezza, e prevedendo mezzi di ricorso e sanzioni per garantirne l'applicazione. Evidenzia che la direttiva, in particolare: stabilisce obblighi per gli Stati membri di adottare una strategia nazionale per la cybersicurezza e di designare autorità nazionali competenti, punti di contatto unici, e gruppi di intervento nazionali per la sicurezza informatica in caso di incidente in ambito nazionale (CSIRT); prevede che gli Stati membri stabiliscano obblighi di gestione e segnalazione dei rischi di cybersicurezza per i soggetti indicati come soggetti essenziali nell'allegato I e come soggetti importanti nell'allegato II e prevede che gli Stati membri stabiliscano obblighi in materia di condivisione delle informazioni sulla cybersicurezza.

Per quanto riguarda le principali novità, sottolinea che la direttiva NIS 2 amplia il campo di applicazione, da un lato, includendovi anche la pubblica amministrazione centrale – lasciando discrezionalità agli Stati membri di inserire gli enti locali in base all'assetto istituzionale –, le piccole e microimprese solo se operano 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, e dall'altro lato, aumentando significativamente i settori di applicazione. Inoltre, mentre ai sensi della precedente direttiva NIS la responsabilità di determinare quali soggetti soddisfacessero i criteri per essere considerati operatori di servizi essenziali spettava agli Stati membri, la nuova direttiva NIS 2 introduce la regola della soglia di dimensione. Ciò significa che tutti i soggetti di medie e grandi dimensioni che operano nei settori o forniscono i servizi contemplati dalla direttiva dovrebbero rientrare nel suo ambito di applicazione. Il nuovo regime esclude dalla sua applicazione i soggetti operanti in settori quali la sicurezza nazionale, la pubblica sicurezza o la difesa, il contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati. Sono altresì esclusi Parlamenti e banche centrali. Inoltre la direttiva NIS 2 prevede l'istituzione di una rete europea delle organizzazioni di collegamento per le crisi informatiche EU-CyCLONe, volta a sostenere la gestione coordinata degli incidenti di cibersicurezza su vasta scala.

Passando alla descrizione del contenuto dell'articolato, segnala che lo schema di decreto legislativo consta di 44 articoli, suddivisi in 6 capi. Rinviando comunque, per un esame più approfondito, alla documentazione predisposta dal Servizio studi, anticipa che provvederà a esaminare sinteticamente i primi tre capi dello schema – e dunque gli articoli da 1 a 22 – lasciando al collega relatore per la IX Commissione la descrizione dei restanti 3 capi, composti dagli articoli da 23 a 44.

Fa presente quindi che il Capo I dello schema di decreto legislativo, composto dagli articoli da 1 a 8, è dedicato alle disposizioni generali. L'articolo 1 stabilisce come oggetto del provvedimento l'individuazione di un livello elevato di sicurezza informatica e preannuncia che tale obiettivo è perseguito attraverso la definizione di una strategia nazionale di cybersicurezza, l'integrazione del quadro di gestione delle crisi informatiche, la conferma dell'Agenzia per la cybersicurezza nazionale (ACN) quale autorità nazionale competente nel settore e la designazione della stessa Agenzia e del Ministero della difesa come autorità nazionali di gestione delle crisi informatiche su vasta scala. L'elevato livello di sicurezza informatica è inoltre perseguito attraverso l'individuazione di autorità di settore che collaborano con l'Agenzia, la determinazione di criteri per l'individuazione dei soggetti cui si applica il provvedimento e la definizione degli obblighi in materia di gestione del rischio informatico e la partecipazione a livello di Unione europea al gruppo di cooperazione NIS tra le autorità competenti in materia, alla Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) e alla rete dei CSIRT nazionali. Evidenzia poi che l'articolo 2 reca le definizioni rilevanti per il provvedimento, che saranno poi esplicitate dal successivo articolato. Per quanto riguarda l'articolo 3, sottolinea che esso definisce l'ambito di applicazione del provvedimento, distinguendo i settori ritenuti, rispettivamente, altamente critici e critici, nonché i relativi sottosettori e tipi di soggetti di cui agli allegati I e II, le categorie delle pubbliche amministrazioni sottoposte alla nuova disciplina, di cui all'allegato III, e le ulteriori tipologie di soggetti a cui si applica il decreto, di cui all'allegato IV. Più nel dettaglio, e rinviando comunque alla ampia documentazione predisposta dal Servizio studi, in base al comma 1, l'allegato I individua i settori ad alta criticità: si tratta di energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile e acque reflue, infrastrutture digitali, gestione dei servizi dell'informazione e della comunicazione. L'allegato II individua gli altri settori critici: servizi postali e di corriere, gestione dei rifiuti, fabbricazione e distribuzione di sostanze chimiche e di alimenti, fabbricazione, servizi digitali e ricerca. L'allegato III individua le amministrazioni pubbliche che rientrano nell'ambito di applicazione del decreto legislativo: si tratta di alcune amministrazioni centrali – organi costituzionali e di rilievo costituzionale, Presidenza del Consiglio dei ministri e i Ministeri, Agenzie fiscali, Autorità amministrative indipendenti –, delle Regioni e delle Province autonome nonché delle amministrazioni locali – città metropolitane, comuni con popolazione superiore a 100.000 abitanti, comuni capoluoghi di regione, ASL – e altri enti pubblici (enti di regolazione dell'attività economica, produttori di servizi economici, a struttura associativa, produttori di servizi assistenziali, ricreativi e culturali, di ricerca e Istituti zooprofilattici sperimentali); in merito sottolinea che il comma 7 dell'articolo 3 prevede che con uno o più decreti del Presidente del Consiglio dei ministri possano essere individuate ulteriori categorie di pubbliche amministrazioni a cui si applica il decreto al fine di adeguare l'elenco di categorie di cui all'allegato III. L'allegato IV, infine, delinea le ulteriori tipologie di soggetti a cui si applica il decreto in esame: soggetti che forniscono servizi di trasporto pubblico locale, istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, società in house, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175. Fa presente poi che, al fine di superare l'attuale disomogeneità nel pro-

cesso di identificazione dei soggetti da parte degli Stati membri, l'articolo 3 introduce, ai commi 2, 3 e 4, il criterio di individuazione dei soggetti su base dimensionale – corrispondente alla cosiddetta « *sizecap rule* » –, estendendo, rispetto al sistema delineato dalla direttiva NIS, l'applicazione della direttiva NIS 2 a tutte le medie e grandi imprese che operano nei settori di cui agli allegati I e II. Alcuni soggetti sono inclusi nell'ambito applicativo del presente schema di decreto indipendentemente dalla loro dimensione, come nel caso di quelli di cui ai commi 5, 6, 9 e 10, delle pubbliche amministrazioni di cui all'allegato III e dei soggetti elencati nell'allegato IV. L'articolo 4 dello schema di decreto legislativo si occupa di esplicitare l'esclusione di una cospicua serie di ambiti dall'applicazione delle norme di recepimento della direttiva NIS2. Sono, quindi, esclusi dall'ambito di applicazione della nuova normativa, nonostante possano essere considerate lato sensu pubbliche amministrazioni, ai sensi del predetto articolo 3, il Parlamento nazionale, l'autorità giudiziaria, la Banca d'Italia e l'UIF. Viene precisato inoltre che gli organi costituzionali e quelli di rilievo costituzionale sono esclusi dall'applicazione del capo V, che inerisce alle misure di monitoraggio, vigilanza ed esecuzione. Ai sensi del comma 3, sono altresì esclusi dalla nuova normativa gli enti, gli organi e le articolazioni della pubblica amministrazione che operano nei settori della pubblica sicurezza; della difesa nazionale, dell'attività di contrasto, compresa l'indagine, l'accertamento e il perseguimento, di reati, gli organismi d'informazione di sicurezza dello Stato e l'ACN. Al comma 4, si attribuisce a una fonte secondaria (uno o più d.P.C.M., d'intesa o su proposta dei Ministri della giustizia, interno e difesa e d'intesa con l'ACN) il compito di individuare quali soggetti siano da ricomprendere nel perimetro di quanti forniscono ai predetti soggetti esclusi beni e servizi in via esclusiva, di modo che costoro, a loro volta, siano esclusi dall'applicazione dei capi IV e V del decreto legislativo in via di approvazione. Al comma 6, è detto – però – che la fornitura esclusiva non dà luogo all'esclusione dall'ambito di applicazione del decreto legislativo se si tratta di attività solo marginalmente connesse a quelle d'istituto dell'organo di cui si tratta; né possono essere esclusi i soggetti fiduciari. Al comma 7 è stabilito un principio generale d'ispirazione e d'interpretazione di tutto il decreto legislativo, in coerenza peraltro con l'art. 346 TFUE: ovunque esso preveda obblighi di ostensione e d'informazione, tali obblighi non possono mai comportare la divulgazione d'informazioni sensibili per gli interessi essenziali dello Stato. Il comma 8 – analogamente – precisa che, laddove la normativa UE o interna preveda lo scambio d'informazioni con la Commissione europea, questo deve avvenire sempre secondo il principio di proporzione e in modo da non pregiudicare gli interessi e la riservatezza dei soggetti essenziali e dei soggetti importanti (designati agli articoli 6, 7, 24 e 30). Passando alla descrizione dell'articolo 5, fa presente che la disposizione individua, sostanzialmente riproducendo il contenuto dell'articolo 26 della direttiva, i criteri per definire a quale giurisdizione siano assoggettati i soggetti, individuati dall'articolo 3, che rientrano nell'ambito di applicazione del presente provvedimento. In particolare, il comma 1 prevede in via generale che tali soggetti sono sottoposti alla giurisdizione nazionale dello Stato membro nel quale sono stabiliti con alcune eccezioni; il comma 2 specifica che si considera stabilimento principale nell'Unione quello dello Stato membro nel quale sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio per la sicurezza informatica. Con riferimento ai fornitori di servizi digitali che non sono stabiliti nell'Unione europea, ma offrono servizi all'interno dell'Unione europea, si prevede l'obbligo di designare un rappresentante nell'Unione europea, che è stabilito in uno di quegli Stati membri in cui sono offerti i servizi (comma 3). Nell'assenza di un rappresentante nell'Unione designato, l'Autorità nazionale competente NIS può avviare un'azione legale nei confronti dei soggetti inadempienti (comma 4). Ai sensi del comma 5 la designazione del rappresentante fa salvi le azioni legali che potrebbero essere

già avviate per violazioni degli obblighi di cui al presente decreto, l'imposizione degli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente (di cui al capo IV) e l'esercizio dei poteri in materia di monitoraggio, vigilanza ed esecuzione (di cui al capo V). L'articolo 6 individua i soggetti essenziali ed i soggetti importanti, in base ai requisiti dimensionali e alla tipologia di prodotti o servizi forniti. Si tratta di categorie che sostituiscono nella direttiva NIS 2 la precedente categorizzazione di « operatori di servizi essenziali » e « fornitori di servizi essenziali », così ampliando il campo di applicazione della direttiva NIS rispetto al passato. Nella categoria dei soggetti essenziali ricadono, ai sensi del comma 1: *a)* i soggetti di cui all'allegato I, ossia i soggetti presenti nei settori ad alta criticità: energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi TIC e spazio, che superano i massimali per le medie imprese; *b)* i soggetti identificati come soggetti critici, indipendentemente dalle loro dimensioni, dallo schema di decreto legislativo A.G. 165, attualmente all'esame della Commissione Affari costituzionali. Rammenta che in base a quello schema il soggetto critico è un soggetto pubblico o privato, appositamente individuato dalle autorità settoriali competenti, fornitore di un servizio essenziale, nei settori di attività cui si riferisce la direttiva. Ulteriori elementi definitori – quale la collocazione del soggetto e della sua infrastruttura critica, in tutto o in parte nel territorio nazionale – si rinvengono nell'articolo 8 dello schema, relativo al procedimento di loro individuazione; *c)* i fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico, che si considerano medie imprese; *d)* i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio, indipendentemente dalle loro dimensioni; *e)* le pubbliche amministrazioni centrali di cui all'allegato III – ovvero organi costituzionali e di rilievo costituzionale; Presidenza del Consiglio dei ministri e Ministeri; agenzie fiscali e autorità amministrative indipendenti – indipendentemente dalle loro dimensioni. Ai sensi del comma 2 ulteriori soggetti essenziali possono essere individuati dall'Autorità nazionale competente NIS, indipendentemente dalle loro dimensioni, tra le pubbliche amministrazioni, i soggetti che forniscono servizi di trasporto pubblico locale, gli istituti di istruzione che svolgono attività di ricerca, i soggetti che svolgono attività di interesse culturale, la società *in house*, le società partecipate e le società a controllo pubblico (come definite nel decreto legislativo n. 175 del 2016), i soggetti delle tipologie di cui agli allegati I, II e IV, indipendentemente dalle loro dimensioni, laddove soddisfino determinati requisiti, le imprese collegate ad un soggetto essenziale o importante, se soddisfano determinati requisiti. Il comma 3 individua, in via residuale, la categoria dei soggetti importanti, facendovi rientrare tutti i soggetti pubblici e privati che rientrano nell'ambito di applicazione del decreto di cui all'articolo 3 che non sono considerati essenziali ai sensi dei commi 1 e 2 dell'articolo in esame. L'articolo 7 delinea il procedimento con cui sono identificati i soggetti importanti ed i soggetti essenziali, prevedendo anzitutto uno scadenzario annuale, in base al quale entro il 28 febbraio di ogni anno i soggetti destinatari delle norme del decreto legislativo sono chiamati a registrarsi su una piattaforma predisposta dall'ACN, indicando una serie d'informazioni identificative del soggetto che si registra. Entro il 31 marzo l'ACN deve compilare l'elenco dei soggetti importanti ed essenziali e comunicare l'inserimento ai soggetti interessati; tra il 15 aprile e il 31 maggio i soggetti inseriti devono comunicare o aggiornare le informazioni inerenti agli aspetti delle comunicazioni elettroniche. Inoltre, la disposizione impone ai soggetti che sono, per definizione, considerati essenziali, a prescindere dall'inserimento negli elenchi, di comunicare all'ACN l'indirizzo della sede principale e delle altre sedi nell'UE o – se si tratti di soggetti extra UE – l'indirizzo e i recapiti della sede del rappresentante in

UE. Le modificazioni delle informazioni già trasmesse sulla piattaforma devono essere comunicate entro 14 giorni dall'avvenuta modifica. Infine, a conclusione del Capo I dello schema di decreto legislativo, fa presente che l'articolo 8 riguarda il trattamento dei dati personali rinviando, quanto alla disciplina applicabile, al codice della *privacy* di cui al decreto legislativo n. 196 del 2003 e alla legislazione dell'Unione europea in materia di trattamento dei dati personali.

Passando alla descrizione del Capo II dello schema di decreto, composto dagli articoli da 9 a 17, fa presente che queste disposizioni sono dedicate al quadro nazionale di sicurezza informatica. In particolare, l'articolo 9 reca disposizioni in materia di strategia nazionale di cybersicurezza, aggiornando, sulla base delle disposizioni della direttiva NIS2, quanto già previsto dall'abrogando decreto legislativo 18 maggio 2018, n. 65, con cui si era data attuazione alla direttiva cosiddetta NIS. In particolare, il comma 1 stabilisce che la Strategia nazionale di cybersicurezza individua obiettivi, risorse e misure per raggiungere e mantenere un alto grado di tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Il comma 2 elenca i contenuti minimi che la Strategia deve contenere, tra i quali in primo luogo obiettivi e priorità soprattutto per i soggetti a rischio, elencati negli allegati I, II, III e IV, del cui contenuto si è dato conto all'articolo 3. Inoltre la Strategia deve contenere, oltre ad un quadro di *governance*: un meccanismo per individuare le risorse e una valutazione dei rischi a livello nazionale; misure volte a garantire la preparazione, la risposta e il recupero da incidenti che comprendano anche la collaborazione tra settori pubblico e privato; un elenco dei soggetti coinvolti nell'attuazione della strategia; un quadro strategico per il coordinamento rafforzato tra le autorità competenti per la condivisione di informazioni sui rischi e per la vigilanza; un piano che contenga misure atte ad incrementare nei cittadini il livello di consapevolezza in materia di cybersicurezza. Il comma 3 elenca le misure strategiche che devono essere contenute nella strategia e che riguardano, tra l'altro la sicurezza informatica nella catena di approvvigionamento dei prodotti e dei servizi TIC (tecnologie dell'informazione e della comunicazione) utilizzati dai soggetti per la fornitura dei loro servizi; l'integrazione di tecnologie avanzate e all'avanguardia nella gestione dei rischi per la sicurezza informatica; la promozione e lo sviluppo di attività di istruzione, di sensibilizzazione e di ricerca in materia di sicurezza informatica, nonché orientamenti sulle buone pratiche e sui controlli destinati ai cittadini, ai portatori di interessi e ad altri soggetti; il sostegno agli istituti accademici e di ricerca per la promozione e la diffusione di infrastrutture e strumenti informatici sicuri; lo sviluppo di procedure adeguate per favorire la condivisione di informazioni tra soggetti nel rispetto del diritto dell'Unione Europea; il rafforzamento dei valori di riferimento relativi alla resilienza e all'igiene informatica delle piccole e medie imprese. Al comma 4 dell'articolo 9, si dispone in ordine alle modalità di valutazione e aggiornamento della Strategia nazionale della cybersicurezza. Rileva poi che l'articolo 10 individua l'Agenzia nazionale per la cybersicurezza come autorità nazionale competente e punto di contatto unico ai fini del provvedimento, specificandone i compiti di vigilanza, regolazione e attuazione. In quanto punto di contatto unico, l'Agenzia svolge una funzione di collegamento per garantire la cooperazione transfrontaliera con gli altri Stati membri, con la Commissione europea e con l'ENISA (Agenzia dell'Unione europea per la Cybersicurezza). Fa presente poi che l'articolo 11, al fine di assicurare l'efficace attuazione del provvedimento in esame, individua le Autorità di settore che supportano l'Autorità nazionale competente e collaborano con essa, specificandone le attribuzioni per i rispettivi settori di competenza. Si tratta della Presidenza del Consiglio e di specifici Ministeri (economia e delle finanze, imprese e *made in Italy*, agricoltura, sovranità alimentare e foreste, ambiente e sicurezza energetica, infrastrutture e trasporti, università e ricerca, cultura, salute), già competenti ai sensi dell'abrogando decreto legislativo n. 65

del 2018. È inoltre previsto che le autorità di settore, per taluni ambiti, si coordinino con le Regioni interessate secondo modalità che verranno stabilite tramite un apposito accordo che andrà definito, entro il 30 settembre 2024, in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano. Ciascuna autorità di settore – con l'eccezione del Ministero dell'economia e delle finanze – è autorizzata a reclutare, con contratto di lavoro subordinato a tempo indeterminato, due unità di personale non dirigenziale, appartenente all'area funzionari. I medesimi soggetti sono autorizzati altresì ad avvalersi di personale non dirigenziale, ad esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche, posto in posizione di comando e di aspettativa, distacco o fuori ruolo ovvero altro analogo istituto previsto dai rispettivi ordinamenti. L'articolo 12, al fine di assicurare l'implementazione e attuazione delle disposizioni del provvedimento, istituisce il Tavolo permanente per l'attuazione della disciplina NIS2 e ne stabilisce la composizione. Il Tavolo ha il compito di: supportare l'Agenzia per la cybersicurezza; formulare proposte e pareri per l'adozione di iniziative, linee guida o atti di indirizzo; predisporre una relazione annuale sull'attuazione provvedimento. L'articolo 13 individua l'Agenzia per la cybersicurezza nazionale e il Ministero della difesa quali Autorità nazionali di gestione delle crisi informatiche. Come previsto dallo schema, tali enti individuano le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi. Si demanda quindi a uno o più decreti del Presidente del Consiglio dei ministri – da adottarsi entro dodici mesi dalla data di entrata in vigore del provvedimento – la definizione del Piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala. Il piano che è aggiornato periodicamente e, comunque, ogni tre anni – stabilisce: obiettivi e misure delle attività nazionali di preparazione; compiti e responsabilità delle due Autorità nazionali; procedure di gestione delle crisi; pertinenti portatori di interessi pubblici e privati; le procedure nazionali e gli accordi tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno e la partecipazione effettivi dell'Italia alla gestione coordinata degli incidenti e delle crisi informatiche su vasta scala a livello dell'UE. Evidenzia che l'articolo 14 dispone che siano assicurate la cooperazione e la collaborazione reciproca tra Agenzia nazionale per la cybersicurezza e l'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazioni (autorità di contrasto), il Garante per la protezione dei dati personali, l'Ente nazionale per l'aviazione civile, l'Agenzia per l'Italia digitale l'Autorità per le garanzie nelle comunicazioni e il Ministero della Difesa, nonché con altre autorità nazionali competenti, per lo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti. Si dispone in particolare che Agenzia per la cybersicurezza e Garante cooperino nei casi di incidenti che comportano violazioni dei dati personali. Si prevede inoltre l'adozione di un decreto del Presidente del Consiglio dei ministri per definire l'elenco dei soggetti – all'interno di quelli individuati annualmente come « essenziali » o « importanti » ai sensi del comma 2 dell'articolo 7 – che impattano sulla efficienza dello Strumento militare e sulla tutela della difesa e sicurezza militare dello Stato, su cui l'Agenzia comunica tempestivamente al Ministero della difesa gli incidenti e le ulteriori informazioni di sicurezza cibernetica. L'articolo 15 reca le funzioni, le dotazioni, i compiti e le forme di collaborazione del gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT Italia), istituito presso l'Agenzia per la cybersicurezza nazionale. Rileva che, come riportato nella relazione illustrativa, l'articolo in esame integra le previsioni della direttiva NIS2 con quanto già disposto dall'abrogando decreto legislativo n. 65 del 2018, nel rispetto dell'articolo 3, comma 1, lettera *e)*, della legge di delegazione europea 2022-2023 che prevede « in relazione all'istituzione del team di risposta agli incidenti di sicurezza informatica (CSIRT), di cui all'articolo 10 della

direttiva (UE) 2022/2555, di confermare le disposizioni dell'articolo 8 del decreto legislativo 18 maggio 2018, n. 65, in materia di istituzione del CSIRT Italia, nonché ampliare quanto previsto dal medesimo decreto legislativo prevedendo la collaborazione tra tutte le strutture pubbliche con funzioni di *Computer Emergency Response Team* (CERT) coinvolte in caso di eventi malevoli per la sicurezza informatica ». L'articolo 16 interviene in materia di divulgazione coordinata delle vulnerabilità. Fa presente al riguardo che con tale formulazione si indica un processo strutturato attraverso il quale le vulnerabilità nei sistemi informatici e di rete sono segnalate al fabbricante o al fornitore dei prodotti TIC (tecnologie dell'informazione e della comunicazione) o dei servizi TIC potenzialmente vulnerabili, in modo tale da consentire loro di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico. Ciò premesso, segnala che l'articolo 16 attribuisce al gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT Italia) il ruolo di coordinatore dei soggetti interessati ai fini della divulgazione coordinata delle vulnerabilità e di intermediario tra la persona fisica o giuridica che segnala la vulnerabilità e il fabbricante o fornitore di servizi TIC o prodotti TIC potenzialmente vulnerabili, su richiesta di una delle parti, prevedendo che sia adottata da parte dell'Autorità nazionale competente una politica nazionale di divulgazione coordinata delle vulnerabilità, tenuto conto degli orientamenti del gruppo di cooperazione NIS. L'articolo 17 disciplina lo scambio volontario di informazioni sulla sicurezza informatica tra i soggetti coinvolti. Questi scambi possono riguardare minacce informatiche, vulnerabilità e raccomandazioni, e sono finalizzati a prevenire incidenti e migliorare la sicurezza informatica. Lo scambio di informazioni avviene tra soggetti essenziali, soggetti importanti e, se opportuno, relativi fornitori, tramite accordi specifici che rispettano la natura sensibile delle informazioni. L'Agenzia per la cybersicurezza nazionale facilita questi accordi, definendo anche gli elementi operativi e supportando i soggetti coinvolti, i quali sono tenuti a notificare la loro partecipazione o il ritiro dagli accordi. È inoltre assicurato l'accesso alle informazioni rilevanti agli organismi di informazione per la sicurezza, di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007 (sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto). Ricorda che all'articolo 4 della legge è disciplinato il Dipartimento delle informazioni per la sicurezza, istituito presso la Presidenza del Consiglio dei ministri, che tra i numerosi compiti: coordina l'intera attività di informazione per la sicurezza; trasmette al Presidente del Consiglio dei ministri le informative e le analisi prodotte da tutto il Sistema di informazione per la sicurezza; raccoglie le informazioni provenienti dai servizi di informazione per la sicurezza, dalle Forze armate e di polizia, dalle amministrazioni dello Stato e da enti di ricerca anche privati. Gli articoli 6 e 7 della legge anzidetta disciplinano rispettivamente l'Agenzia informazione e sicurezza esterna e l'Agenzia informazioni e sicurezza interna. Le Agenzie citate effettuano il concreto compito di ricerca ed elaborazione delle informazioni utili alla sicurezza della Repubblica.

Per quanto riguarda il contenuto del Capo III dello schema di decreto legislativo, composto dagli articoli da 18 a 22, e dedicato alla cooperazione a livello dell'Unione europea e internazionale, fa presente che l'articolo 18 disciplina l'attività del Gruppo di cooperazione NIS, già operante ai sensi dell'abrogando decreto legislativo n. 65 del 2018, prevedendo che l'Autorità nazionale competente NIS partecipi alle attività del Gruppo avvalendosi, se lo richiede, del supporto delle Autorità di settore NIS sulla base delle loro specifiche competenze. Più nel dettaglio, e rinviando comunque alla documentazione predisposta dal Servizio studi, evidenzia che la direttiva (UE) 2022/2555 ha istituito all'articolo 14 il Gruppo di cooperazione, costituito dai rappresentanti degli Stati Membri, della Commissione europea e dell'Agenzia dell'UE per la sicurezza delle reti e dell'informazione (ENISA), con il compito di implementare la coope-

razione strategica e lo scambio di informazioni tra gli Stati membri rafforzandone la fiducia reciproca. Lo schema di decreto legislativo di recepimento prevede, in tal senso, al comma 1 dell'articolo 18, che sia l'Autorità nazionale competente NIS, ovvero l'Agenzia per la cybersicurezza, a partecipare al Gruppo di cooperazione NIS. A norma del comma 2, inoltre, possono essere chiamate a collaborare con l'Autorità nazionale competente NIS anche le Autorità di settore NIS, ovvero la Presidenza del Consiglio dei Ministri e i singoli Ministeri, per i rispettivi ambiti di competenza. Ai fini della loro partecipazione alle attività del Gruppo, secondo il comma 3, l'Autorità nazionale competente NIS e, a suo supporto, le Autorità di settore NIS, provvedono a una serie di attività, tra cui: tenere conto degli orientamenti non vincolanti del Gruppo in merito al recepimento e all'attuazione della direttiva (UE) 2022/2555 (lettera *a)*) e di quelli relativi alle politiche in materia di divulgazione coordinata delle vulnerabilità di cui è competente il CSIRT Italia (lettera *b)*); discutere sui casi di assistenza reciproca (lettera *g)*) e, su impulso di uno o più Stati, discutere le richieste di assistenza reciproca di cui è competente l'Autorità nazionale competente NIS (lettera *h)*); scambiare opinioni su misure per mitigare i rischi su vasta scala sulla base degli insegnamenti tratti da EU-CyCLONe e dalla Rete di CSIRT nazionali (lettera *l)*); partecipare se necessario ai programmi di sviluppo delle capacità anche prevedendo scambi tra il personale delle Autorità nazionali dei diversi Stati membri (lettera *m)*). Il comma 4 dell'articolo 18 specifica che, sempre ai fini della partecipazione alle attività del Gruppo di cooperazione, l'Autorità nazionale competente NIS, con la collaborazione delle Autorità di settore NIS interessate, contribuisce, in particolare: alla definizione degli orientamenti non vincolanti di cui alle lettere *a)* e *b)* del precedente comma (lettere *a)* e *b)*); alla definizione di pareri non vincolanti e alla cooperazione con la Commissione europea sulle nuove iniziative strategiche in materia di sicurezza informatica (lettera *c)*), nonché sui progetti di atti delegati o di esecuzione di cui è competente la Commissione europea sulla base della stessa direttiva (lettera *d)*); alla definizione degli orientamenti strategici delle due reti di cui sopra, ovvero EU-CyCLONe e la Rete CSIRT nazionali su specifiche questioni emergenti (lettera *h)*); al rafforzamento delle capacità di sicurezza informatica a livello europeo (lettera *i)*); all'organizzazione di riunioni congiunte e periodiche con i portatori di interessi competenti del settore privato dell'Unione europea per discutere le attività dal Gruppo di cooperazione NIS traendone contributi (lettera *l)*); alla definizione della metodologia per la revisione tra pari già menzionata e di quella relativa all'autovalutazione per gli Stati e all'elaborazione di codici di condotta per gli esperti di cybersicurezza che sono selezionati, ai sensi dell'articolo 21, comma 2, lettera *b)*, dall'Autorità nazionale competente NIS, sentito il Tavolo per l'attuazione della disciplina NIS, con una o più deliberazioni come stabilisce l'articolo 40, comma 5, dello schema di decreto in esame (lettera *m)*); alla collaborazione con l'ENISA e con la Commissione europea per la pubblicazione della relazione biennale sullo stato della sicurezza informatica dell'Unione, che viene poi presentata al Parlamento europeo a norma dell'articolo 18 della direttiva (UE) 2022/2555 (lettera *p)*), nonché alla collaborazione con l'ENISA, con la Commissione e con la Rete CSIRT nazionali per una definizione della metodologia relativa alla valutazione sul livello di capacità, risorse e strategie di cybersicurezza e sull'allineamento delle strategie nazionali, come disciplinato dall'articolo 18, paragrafo 3, della direttiva europea allo scopo di redigere la relazione biennale di cui sopra (lettera *q)*). Il successivo articolo 19 disciplina la partecipazione dell'Agenzia per la cybersicurezza nazionale, quale Autorità nazionale di gestione delle crisi informatiche, alla Rete delle organizzazioni di collegamento per le crisi informatiche EU-CyCLONe. A tal fine, in base al comma 2, l'Agenzia contribuisce, in particolare: ad aumentare il livello di preparazione per la gestione di incidenti e crisi informatiche su vasta scala, a sviluppare una conoscenza condivisa sui

medesimi eventi, a valutarne le conseguenze e proporre misure di attenuazione, nonché a coordinarne la gestione e sostenere il processo decisionale politico in materia (lettere da *a)* a *d)*); a discutere, su richiesta di uno Stato membro, i piani nazionali di risposta agli incidenti e alle crisi informatiche su vasta scala previsti dall'articolo 9, paragrafo 4, della direttiva oggetto di recepimento (lettera *e)*); in relazione a tale previsione, il comma 3 specifica poi che anche l'Agenzia può richiedere di discutere il piano nazionale; a supportare la collaborazione con il gruppo di cooperazione NIS, a cooperare con la rete di CSIRT nazionali e a predisporre la relazione al Parlamento europeo e al Consiglio sui lavori della Rete (lettere da *f)* ad *h)*). Rileva poi che l'articolo 20 regola la partecipazione del CSIRT Italia alla rete di CSIRT nazionali. A tale fine, al comma 2 si dispone che il CSIRT Italia contribuisca, tra gli altri aspetti, a: scambiare una serie di informazioni, indicate dalle lettere da *a)* a *f)*; su richiesta di un membro della Rete di CSIRT nazionali, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro, e fornire assistenza ai CSIRT nazionali di altri Stati membri nel far fronte a incidenti che interessano due o più Stati membri (lettere *g)* ed *h)*); cooperare e scambiare migliori pratiche con i CSIRT nazionali designati dagli altri Stati membri in qualità di coordinatori ai sensi dell'articolo 12 della direttiva (UE) 2022/2555, nonché fornire loro assistenza per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro (lettera *i)*); discutere e individuare ulteriori forme di cooperazione operativa (lettera *l)*), come ulteriormente specificato dalla stessa lettera; informare il Gruppo di cooperazione NIS sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera *i)* e, se necessario, chiedere orientamenti non vincolanti in merito (lettera *q)*); fornire, infine, orientamenti non vincolanti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa (lettera *s)*). Il successivo articolo 21 disciplina una procedura di revisione delle modalità attuative della direttiva NIS 2 – in particolare per questioni specifiche di natura transfrontaliera o intersettoriale – denominata « revisione tra pari » ai sensi dell'articolo 19 della direttiva NIS 2. In particolare, il comma 1 distingue due modalità di partecipazione alla procedura di revisione da parte dell'ACN – Autorità nazionale competente NIS (nel quadro della metodologia di cui all'articolo 18, comma 4, lettera *m)*, del presente provvedimento): da un lato, richiedendo l'esecuzione di una revisione tra pari in relazione all'attuazione della direttiva a livello nazionale (lettera *a)*); dall'altro, indicando uno o più rappresentanti dell'ACN o delle Autorità di settore NIS quali esperti di sicurezza informatica per eseguire revisioni tra pari presso altri Stati membri, su richiesta di questi ultimi, nel rispetto dei codici di condotta. Eventuali rischi di conflitto di interessi riguardanti gli esperti di sicurezza informatica designati sono condivisi con gli altri Stati membri, il Gruppo di cooperazione NIS, la Commissione europea e l'ENISA prima dell'inizio della revisione tra pari (lettera *b)*). Nel primo caso, ossia quando la revisione è richiesta dall'ACN – Autorità nazionale NIS, questa, con propria determinazione (comma 2): individua almeno un aspetto da sottoporre alla revisione tra pari (lettera *a)*), tra quelli indicati dalla medesima lettera; notifica, prima dell'inizio della revisione tra pari, agli Stati membri partecipanti, l'ambito di applicazione della medesima, comprese le questioni specifiche individuate (lettera *b)*); effettua un'autovalutazione degli aspetti oggetto della revisione (lettera *c)*); seleziona, tra gli esperti di sicurezza informatica indicati dagli altri Stati membri partecipanti, gli esperti idonei da designare. Qualora l'ACN – Autorità nazionale competente NIS si opponga alla designazione di uno o più esperti indicati, comunica allo Stato membro indicante i motivi debitamente giustificati (lettera *d)*); fornisce l'autovalutazione di cui sopra agli esperti designati (lettera

e)); fornisce agli esperti designati le informazioni necessarie per la valutazione (lettera *f)*); formula osservazioni sulla relazione elaborata dagli esperti designati (lettera *g)*); può pubblicare la relazione elaborata dagli esperti designati (lettera *h)*). Nel secondo caso, ossia quando la revisione è promossa da altri Stati membri, il comma 3 individua alcuni compiti e obblighi in capo agli esperti di sicurezza informatica partecipanti alla revisione indicati dall'Autorità nazionale competente NIS. In particolare, questi: non devono divulgare a terzi le eventuali informazioni sensibili o riservate ottenute nel corso delle revisioni (lettera *a)*); partecipano alle attività necessarie allo svolgimento delle revisioni tra pari tramite visite in loco fisiche o virtuali e scambi di informazioni a distanza (lettera *b)*); contribuiscono all'elaborazione delle relazioni sui risultati e sulle conclusioni delle revisioni tra pari (lettera *c)*). Infine, ai sensi del comma 4, la condivisione delle informazioni è effettuata nel rispetto della legislazione nazionale e dell'Unione europea in materia di tutela delle informazioni protette da classifica di segretezza e di salvaguardia delle funzioni essenziali dello Stato, compresa la sicurezza nazionale. Infine, fa presente che l'articolo 22 individua gli obblighi di comunicazione nei confronti dell'Unione europea da parte rispettivamente della Presidenza del Consiglio dei ministri, dell'Agenzia per la cybersicurezza nazionale, in qualità di Autorità nazionale competente e Punto di contatto unico NIS, nonché di Autorità nazionale di gestione delle crisi cibernetiche. In primo luogo, ai sensi del comma 1, dopo l'entrata in vigore del decreto in esame, la Presidenza del Consiglio dei ministri deve notificare tempestivamente alla Commissione europea tutte le designazioni delle autorità competenti. Pertanto: la conferma dell'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS e quale Punto di contatto unico NIS; la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e del Ministero della difesa, quali Autorità nazionali di gestione delle crisi informatiche, e i relativi ambiti di competenza come indicati all'articolo 2, comma 1, lettera *g)*. Ogni successiva ulteriore modifica a tali designazioni o compiti deve essere ulteriormente notificata, senza ingiustificato ritardo. Alle designazioni sono assicurate idonee forme di pubblicità. In secondo luogo, ai sensi del comma 2, l'Agenzia per la cybersicurezza nazionale, in qualità di autorità nazionale competente, trasmette alla Commissione europea la Strategia nazionale di cybersicurezza e i suoi aggiornamenti. Inoltre ha una serie di obblighi di comunicazione alla Commissione relativi al numero dei e ad informazioni sui soggetti essenziali e su quelli importanti individuati a livello nazionale (ivi incluse le misure sanzionatorie e le disposizioni sulle sanzioni). Infine alcune informazioni sui soggetti essenziali e sui soggetti importanti devono essere comunicate all'ENISA, ai fini del loro inserimento nel registro di cui all'articolo 27 della direttiva (UE) 2022/2555. L'Autorità nazionale competente NIS può richiedere ad ENISA l'accesso a tale registro, assicurando la tutela della riservatezza delle informazioni ivi contenute. In terzo luogo, l'Agenzia per la cybersicurezza nazionale, in qualità di Punto di contatto unico NIS (comma 3) comunica alla Commissione europea le designazioni relative al CSIRT Italia, anche quale coordinatore in materia di divulgazione delle vulnerabilità, con i relativi compiti. Inoltre trasmette all'ENISA: una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti, con cadenza trimestrale a partire dal 1° gennaio 2026; senza ingiustificato ritardo, le notifiche di incidente con effetti transfrontalieri di cui agli articoli 25 e 26 (la trasmissione è prevista anche ai punti di contatto unici degli altri Stati membri interessati). Infine, ai sensi del comma 4, in qualità di Autorità nazionale di gestione delle crisi informatiche, l'Agenzia comunica alla Commissione europea e alla Rete europea delle organizzazioni di collegamento per le crisi informatiche (EUCyCLONe) entro tre mesi dall'adozione o dall'aggiornamento del Piano nazionale di risposta agli incidenti e alle crisi informatiche su larga scala, le informazioni del

Piano, fatto salvo quanto previsto dall'articolo 4, commi 1, 6 e 7, che stabilisce alcuni limiti al campo di applicazione dello schema di decreto in esame.

Enzo AMICH (FDI), *relatore per la IX Commissione*, riferisce sulla parte di schema di decreto legislativo contenuta nei capi IV, V e VI.

Per completezza ricorda che, come accennato dal collega Russo, i soggetti importanti e i soggetti essenziali, ai fini della direttiva NIS-2, sono definiti e identificati negli articoli 6 e 7 del provvedimento e secondo le procedure ivi descritte.

In particolare, il capo IV del decreto in esame è dedicato agli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente.

L'articolo 23 – con il quale si apre il capo IV – prevede gli obblighi cui sono chiamati gli organi amministrativi e direttivi di tali soggetti.

Si tratta in sostanza dei consiglieri d'amministrazione, degli amministratori delegati e dei dirigenti di strutture operative.

Costoro devono approvare modalità di gestione dei rischi e verificare che le misure previste per tale gestione siano correttamente eseguite. Essi devono altresì vigilare affinché lo scadenzario temporale previsto dall'articolo 7 sia rispettato.

Onde poter adempiere efficacemente a questi obblighi, gli organi direttivi e amministrativi devono seguire un corso di formazione in sicurezza informatica e devono fornire simile formazione professionale per i loro dipendenti, affinché costoro siano capaci di individuare i rischi e valutare le pratiche di gestione di tali rischi.

L'articolo 24 elenca con maggiore puntualità in che cosa consistano le misure di gestione del rischio, le quali comprendono, per esempio, politiche di analisi dei rischi, la manutenzione dei sistemi informativi e di rete, pratiche di igiene di base e di formazione in materia di sicurezza informatica e diffusione tra il personale di soluzioni di autenticazione a più fattori per l'accesso ai sistemi.

L'articolo 25 prevede gli obblighi di notifica degli incidenti al CSIRT (vale a dire, ricorda, il Gruppo nazionale di risposta agli incidenti, previsto dall'articolo 10 della direttiva NIS-2). In pratica, è fatto obbligo ai soggetti essenziali e soggetti importanti di pre-notificare immediatamente – entro 24 ore – gli incidenti significativi. Entro 72 ore devono notificare al CSIRT tali incidenti, indi, essi devono successivamente produrre, su eventuale richiesta, una relazione intermedia ed entro un mese, una relazione finale sull'incidente, contenente la descrizione dettagliata dello stesso, il tipo di minaccia o la causa originale, le misure di attenuazione e l'eventuale impatto transfrontaliero.

Sottolinea, inoltre, che per i servizi fiduciari (vale a dire, quei servizi di autenticazione e convalida delle firme digitali ed elettroniche), invece, entro le 24 ore deve essere fatta direttamente la notifica completa dell'incidente, con la valutazione del suo impatto sul sistema informatico gestito. Questa deroga si comprende alla luce della particolare delicatezza dei dati gestiti.

La notifica, in ogni caso, fa scattare due ulteriori serie di flussi informativi: uno dal CSIRT al soggetto segnalante e uno da quest'ultimo agli utenti.

Il CSIRT fornisce adeguate informazioni su come procedere nella gestione dell'incidente; i soggetti che hanno subito un incidente significativo devono metterne al corrente gli utenti fruitori del servizio. Peraltro, nei casi più gravi, l'ACN informa il pubblico generale per metterlo in guardia e per dare indicazioni su come evitare ulteriori incidenti.

Mentre l'articolo 26 prevede la possibilità di notifiche volontarie per accadimenti diversi dagli incidenti significativi, l'articolo 27 prevede il potere dell'ACN di imporre ai soggetti essenziali e ai soggetti importanti di utilizzare determinati prodotti, procedure e protocolli volti a contenere i rischi informatici.

L'articolo 28 attribuisce all'ACN il compito di promuovere l'uso di specifiche tecniche, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, nonché di predisporre e aggiornare periodicamente un elenco delle categorie di tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di ge-

stione dei rischi per la sicurezza informatica, tenendo conto delle linee guida e degli orientamenti non vincolanti elaborati da ENISA.

Ritiene che le Commissioni potrebbero suggerire al Governo di rafforzare il contenuto di tale previsione, attribuendo all'ACN altresì il compito di individuare puntualmente le misure minime che i soggetti devono adottare per essere considerati adempienti ai sensi degli articoli 24 e 28, in modo che gli operatori possano conoscere con esattezza a quali criteri tecnologici attenersi onde evitare di essere sanzionati.

L'articolo 29 prevede che i gestori di registri e i fornitori di servizi di registrazione di domini di primo livello raccolgano e mantengano accurati dati di registrazione, che devono includere, tra l'altro: nome di dominio, data di registrazione, contatti del registrante e amministratore (nome, email, telefono).

Inoltre, impone l'obbligo, previa richiesta motivata, di fornire i dati di registrazione specifici entro 72 ore. A tal fine, l'ACN può richiedere l'accesso ai dati e stipulare protocolli con i gestori e fornitori. Infine, specifica che onde evitare duplicazioni, gestori e fornitori devono collaborare nella raccolta e mantenimento dei dati.

L'articolo 30, a sua volta, prevede che tra il 1° maggio e il 30 giugno di ciascun anno, i soggetti essenziali e i soggetti importanti che abbiano avuto la comunicazione di essere stati inseriti nell'apposito registro ai sensi dell'articolo 7, comunicano e aggiornano un elenco delle proprie attività e dei propri servizi. In pratica, si tratta di un completamento degli obblighi già previsti all'articolo 7.

Gli articoli 31 e 32, tenuto conto che l'ACN con proprio provvedimento, ai sensi dell'articolo 40, stabilisce le modalità di adempimento degli obblighi fissati in tutto il testo dello schema di decreto, statuiscono però che questo potere regolamentare debba essere esercitato secondo proporzione e gradualità, anche con riferimento a settori specifici.

L'articolo 33 contiene disposizioni di coordinamento con la normativa nazionale relativa al Perimetro di sicurezza nazionale cibernetica, in particolare per quel che concerne la disciplina sugli obblighi dei soggetti e dei loro rispettivi sistemi informativi, reti e servizi informatici.

Con l'articolo 34 si apre il capo V, che, in generale, inerisce ai poteri di vigilanza e monitoraggio dell'ACN nei confronti dei soggetti essenziali e dei soggetti importanti.

In via di estrema sintesi, il potere di vigilanza si esercita, come accennato – ai sensi degli articoli 35, 36 e 37 – in via regolamentare, ma anche in via cartolare sulla base delle informazioni fornite dagli operatori e ispettiva mediante ispezioni in loco.

All'articolo 38 è previsto altresì un potere sanzionatorio, il quale può essere esercitato in presenza di una gamma ampia di inadempimenti degli obblighi poc'anzi descritti. Sono previste sanzioni amministrative pecuniarie e, per i soggetti responsabili che siano anche pubblici dipendenti, è prevista la responsabilità disciplinare oltre che amministrativo-contabile. Per i soggetti importanti e essenziali che non siano pubbliche amministrazioni, i commi 9 e successivi dell'articolo 38 prevedono anche il calcolo della misura della sanzione come percentuale sulla base del fatturato annuo. È previsto anche il caso della recidiva.

L'articolo 39 disciplina le modalità di cooperazione e assistenza reciproca tra l'ACN e le Autorità competenti degli altri Stati membri.

Con l'articolo 40 si apre il capo VI, dedicato alle disposizioni finali e transitorie. Tale articolo prevede l'adozione di decreti del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge n. 400 del 1988, il quale – come è noto – prevede il potere regolamentare del Governo. Tale potere prevede l'emanazione del regolamento attuativo di leggi, decreti legislativi, o fonti unionali con decreto del Presidente della Repubblica (articolo 17, comma 1).

Qui, invece, ai commi 1, 2 e 3 si prevede l'adozione di decreto del Presidente del Consiglio dei ministri, tra l'altro, per stabilire le modalità e le procedure di vigilanza dell'ACN ai sensi del citato articolo 34; individuare le modalità di esercizio del

potere sanzionatorio; identificare le modalità di raccordo e di collaborazione tra l'ACN e le autorità NIS di settore. Ai commi 4 e 5 è prevista invece la determinazione dell'ACN, tra l'altro per stabilire l'elenco dei soggetti essenziali e dei soggetti importanti, di cui all'articolo 7, che, ai sensi del comma 6 dell'articolo 40, è sottratto all'accesso del pubblico.

Dall'articolo 41 all'articolo 44 sono previste norme transitorie, abrogazioni, sostituzioni e la copertura finanziaria.

In definitiva, si tratta di una materia delicata e complessa, che ha anche nessi con l'intelligenza artificiale, poiché lo sviluppo di quest'ultima deve poter contare su *dataset* protetti e integri.

In virtù di tale importanza e delicatezza, prospetta alle Commissioni riunite l'opportunità di svolgere un breve ciclo di audizioni o comunque di richiedere memorie scritte sul tema.

Per ogni ulteriore approfondimento sul contenuto del provvedimento, rinvia alla documentazione predisposta dagli uffici.

Giulia PASTORELLA (AZ-PER-RE) ringrazia i relatori per aver espresso la volontà di intraprendere un lavoro congiunto sul provvedimento in esame, che nonostante il carattere tecnico risulta connotato da un'elevata importanza strategica.

Si riserva di presentare dei suggerimenti in merito ad alcuni punti specifici. In particolare, rileva una prima criticità sull'articolo 4, per l'esclusione di una serie di soggetti dall'elencazione di cui all'articolo 3.

Giudica favorevolmente la proposta di intraprendere un ciclo di audizioni e di richiedere memorie scritte.

Critica, tuttavia, il fatto che il Governo abbia deciso di anticipare alcuni argomenti con l'adozione, nel mese di maggio dell'anno in corso, del decreto-legge sulla cybersicurezza. In particolare, ricorda di aver segnalato, in quella sede, la circostanza che il suddetto decreto trattasse la materia in maniera incompleta, considerando la questione relativa all'obbligo di notifica ma non anche la questione sulla prevenzione del rischio, di cui agli articoli 23 e successivi del provvedimento in esame, nonché le necessità di un intervento organico sulla materia quale appunto quello relativo completa attuazione della direttiva NIS2.

Ritiene, pertanto, che l'adozione del decreto cybersicurezza abbia aggravato il lavoro delle pubbliche amministrazioni, che si troveranno a breve ad applicare una nuova normativa sulla stessa materia e che non hanno potuto disporre, fin dall'inizio, di un quadro chiaro e completo.

Andrea CASU (PD-IDP) giudica favorevolmente la decisione di intraprendere un lavoro congiunto ed esprime piena disponibilità in tal senso, ricordando che la IX Commissione non è stata coinvolta nel processo che ha portato all'adozione del decreto-legge sulla cybersicurezza.

In relazione alla questione avanzata dalla collega Pastorella, rileva che la decisione del Governo di anticipare alcuni argomenti all'interno del decreto-legge sulla cybersicurezza era legata all'esigenza di annunciare tale iniziativa in occasione del G7.

Un'ulteriore motivazione, che tuttavia non è stata fatta propria dal Governo, era rappresentata dalla necessità di irrobustimento del sistema di cybersicurezza italiano, che avrebbe consentito di ricevere ulteriori risorse, strumenti e opportunità da impiegare nel settore della cybersicurezza. Infatti, sebbene la strategia nazionale per la cybersicurezza contempli un finanziamento pari all'1,2 per cento degli investimenti nazionali lordi su base annuale, tale impegno è oggi ampiamente disatteso dal Governo.

Inoltre, giudica negativamente la circostanza che la materia sia stata frammentata all'interno di diversi provvedimenti, osservando che questo non soltanto non consente di raggiungere i risultati sperati, ma al contrario genera confusione tra gli operatori chiamati ad applicare la normativa.

Propone, infine, di predisporre un'agenda di lavoro che consenta di realizzare un intervento normativo chiaro e completo, anche attraverso un ciclo di audizioni e il necessario confronto fra le forze politiche.

Nazario PAGANO, *presidente della I Commissione*, nel sottolineare i numerosi prov-

vedimenti attualmente all'esame della I Commissione e la prevista mole di lavoro parlamentare nel periodo che precede la chiusura estiva, evidenzia l'opportunità di circoscrivere la fase conoscitiva, procedendo non ad audizioni informali ma alla richiesta di memorie scritte.

Matteo MAURI (PD-IDP), in relazione alla proposta formulata dal Presidente Pagano, e pur nella consapevolezza dell'ingorgo di provvedimenti del mese di luglio, fa presente che la conversione di numerosi decreti-legge non può pregiudicare l'approfondimento di un provvedimento complesso come quello all'esame delle Commissioni. Non ritiene dunque opportuno escludere completamente le audizioni informali e propone, per andare comunque incontro alle esigenze prospettate dal Presidente Pagano, di circoscrivere le audizioni informali a quelle di tre, quattro auditi particolarmente autorevoli, chiedendo a tutti gli altri esperti una memoria scritta.

Nazario PAGANO, *presidente della I Commissione*, afferma di rispettare profondamente le esigenze di approfondimento istruttorio e che dunque, se si conviene di trovare spazi anche fuori dagli ordinari giorni dedicati ai lavori parlamentari, la proposta di mediazione dell'onorevole Mauri può essere accolta. Rammenta comunque che mentre delle audizioni informali resta traccia solo attraverso la trasmissione via *web*, le memorie scritte restano agli atti delle Commissioni.

Giulia PASTORELLA (AZ-PER-RE) non esprime contrarietà all'opportunità di richiedere soltanto memorie scritte. Tuttavia, evidenzia i benefici che derivano dallo svolgimento delle audizioni informali, nel corso delle quali è possibile instaurare un confronto diretto e dinamico che, data la delicatezza e l'importanza del provvedimento, risulta opportuno e necessario.

Salvatore DEIDDA, *presidente*, propone di predisporre un calendario sulla base delle segnalazioni dei Gruppi parlamentari, che dovranno pervenire entro lunedì 8 luglio, procedendo ad una rigorosa selezione delle audizioni da svolgere.

Nessun altro chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 13.50.