# XIV COMMISSIONE PERMANENTE

## (Politiche dell'Unione europea)

*S O M M A R I O*



### SEDE CONSULTIVA

*Mercoledì 8 maggio 2024. — Presidenza del presidente Alessandro GIGLIO VIGNA.*

**La seduta comincia alle 12.45.**

**Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.**

**C. 1717 Governo.**

(Parere alle Commissioni I e II).

*(Esame e conclusione – Parere favorevole).*

La Commissione inizia l'esame del provvedimento.

Alessandro GIGLIO VIGNA, *presidente e relatore*, riferisce che il disegno di legge all'esame della Commissione, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, si pone l'obiettivo di prevenire minacce perpetrate con mezzi telematici e informatici e di realizzare una più intensa tutela della sicurezza cibernetica.

La materia della sicurezza cibernetica è regolata a livello dell'Unione europea dalla direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. direttiva NIS – *Network and Information Security*) che reca misure per 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 interno con il decreto legislativo n. 65 del 18 maggio 2018, che costituisce la cornice legislativa 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.

La normativa europea è stata aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 (c.d. direttiva NIS 2) che ha sostituito 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 cybersicurezza.

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. La delega per la trasposizione della direttiva nel diritto interno è contenuta nella di legge di delegazione europea 2022-2023 (legge 21 febbraio 2024, n. 15).

Venendo ai contenuti dell'articolato, l'articolo 1 prevede un obbligo di segnalazione su alcune tipologie di incidenti aventi un impatto su reti e sistemi informatici in capo alle pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni, alle regioni e province autonome, ai comuni con popolazione superiore a 10.000 abitanti e ai comuni capoluoghi di regione, alle società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti, alle aziende sanitarie locali, alle società *in house* degli enti qui richiamati.

L'articolo 2 stabilisce l'obbligo di adottare gli interventi risolutivi in conseguenza delle segnalazioni che l'Agenzia per la cybersicurezza nazionale (ACN) effettua circa specifiche vulnerabilità. Tale articolo prevede inoltre l'applicazione di sanzioni per la mancata o ritardata adozione dei richiamati interventi nonché una causa di esclusione dall'applicazione delle sanzioni medesime nel caso in cui motivate esigenze di natura tecnico-organizzativa, tempestivamente comunicate all'ACN, impediscano l'adozione degli interventi opportuni o ne comportino il differimento oltre il termine indicato.

L'articolo 3 modifica l'articolo 1, comma 3-*bis*, del decreto-legge 21 settembre 2019, n. 105 (c.d. Decreto Perimetro), per finalità di raccordo e coordinamento con le disposizioni recate dal presente disegno di legge.

L'articolo 4 prevede la possibilità di far partecipare alle riunioni del Nucleo per la cybersicurezza ulteriori soggetti quali rappresentanti della Direzione nazionale antimafia e antiterrorismo e rappresentanti della Banca d'Italia, in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese.

L'articolo 5 consente al Presidente del Consiglio dei Ministri di disporre il differimento degli obblighi informativi e delle attività di resilienza in capo all'ACN nei casi in cui questo sia considerato strettamente necessario dai servizi di sicurezza della Repubblica.

L'articolo 6 reca norme che mirano al rafforzamento della resilienza delle pubbliche amministrazioni, istituendo all'interno di esse la struttura preposta alle attività di cyber-sicurezza, nonché del referente per la cyber-sicurezza, unico punto di contatto delle amministrazioni coinvolte con l'ACN.

L'articolo 7 è volto a conferire all'ACN la funzione intesa a promuovere e valorizzare il ruolo dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale.

L'articolo 8 prevede la possibilità di adottare con decreto del Presidente del Consiglio dei Ministri, sentito il Comitato interministeriale per la cybersicurezza, un regolamento per la disciplina del procedimento sanzionatorio amministrativo dell'ACN che stabilisca, in particolare, termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicu-

rezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia.

L'articolo 9 stabilisce un divieto, della durata di due anni, di assunzione, anche di incarichi, presso soggetti privati finalizzata allo svolgimento di mansioni in materia di cybersicurezza per i dipendenti appartenenti al ruolo del personale dell'Agenzia che abbiano partecipato a specifici percorsi formativi di specializzazione. Vengono tuttavia previste delle specifiche cause di esclusione dall'applicazione del richiamato divieto.

L'articolo 10 reca disposizioni dirette a indicare criteri di cybersicurezza in tema di appalti pubblici. In particolare, è prevista l'adozione di un decreto del Presidente del Consiglio dei ministri, entro centoventi giorni dalla data di entrata in vigore della legge, su proposta dell'ACN, previo parere del Comitato interministeriale per la cybersicurezza, con cui sono individuati gli elementi essenziali di cybersicurezza da tenere in considerazione in relazione alle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso.

L'articolo 11 reca modifiche al codice penale in materia di prevenzione e contrasto dei reati informatici, intervenendo sul sistema delle aggravanti per quanto riguarda in particolare il delitto di accesso abusivo ad un sistema informatico e il delitto di detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

L'articolo 12 contiene le modifiche al codice di procedura penale consequenziali rispetto agli interventi di prevenzione e contrasto dei reati informatici introdotti dall'articolo 11, prevedendo in particolare l'attribuzione della competenza sulle indagini alla Procura distrettuale; la deroga al regime in materia di proroga delle indagini preliminari; termini di durata massima di due anni per lo svolgimento delle suddette indagini.

L'articolo 13 prevede alcune modifiche alle disposizioni del codice di procedura penale relative ai soggetti che collaborano con la giustizia, allo scopo di estendere il campo di applicazione della relativa disciplina agli autori dei reati informatici di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale.

Nella prospettiva del potenziamento degli strumenti investigativi, l'articolo 14 estende l'applicazione della disciplina delle intercettazioni prevista per i reati di criminalità organizzata anche ai reati informatici rimessi al coordinamento del Procuratore nazionale antimafia e antiterrorismo.

L'articolo 15 interviene, poi, in materia di responsabilità amministrativa degli enti per gli illeciti dipendenti da reato informatico, modificando sul punto l'articolo 24-*bis* del decreto legislativo 8 giugno 2001, n. 231.

L'articolo 16 concerne il procedimento di applicazione delle speciali misure di protezione per i testimoni di giustizia e per gli altri protetti, stabilendo che la Commissione centrale debba richiedere il parere al Procuratore nazionale antimafia e antiterrorismo sulla proposta di ammissione alle speciali misure, anche nel caso dei gravi delitti informatici indicati nell'articolo 371-*bis*, comma 4-*bis*, c.p.p.

L'articolo 17 è invece dedicato alla regolazione dei rapporti i tra l'ACN, il Procuratore nazionale antimafia e antiterrorismo, la Polizia giudiziaria e il Pubblico ministero, realizzata intervenendo sull'articolo 17 del decreto-legge 14 giugno 2021, n. 82.

L'articolo 18 reca infine la clausola di invarianza finanziaria, disponendo in particolare al comma 2 che i proventi delle sanzioni previste nei casi di reiterata inosservanza dell'obbligo di notifica degli incidenti di sicurezza informatica e degli attacchi informatici, siano destinati alle entrate dell'Agenzia.

Alla luce delle varie iniziative assunte in ambito europeo l'impianto complessivo del provvedimento risponde in modo adeguato ed efficace alla complessità e rapidità degli scenari di crisi, rafforzando il ruolo istituzionale dell'ACN anche in relazione alle sfide dell'attuale contesto caratterizzato da nuove tipologie di confronto ibrido come emerso nel corso dell'ampio ciclo di audi-

zioni dedicato dalla XIV Commissione all'esame della Comunicazione congiunta della Commissione e dell'Alto Rappresentante per gli affari esteri e la politica di sicurezza dell'UE, sulla politica di cyberdifesa dell'UE.

Evidenzia conclusivamente che il disegno di legge non presenta incompatibilità con l'ordinamento dell'Unione europea.

Illustra una proposta di parere favorevole *(vedi allegato)*.

Nessun altro chiedendo di intervenire, la Commissione approva la proposta di parere.

**La seduta termina alle 12.50.**

**UFFICIO DI PRESIDENZA INTEGRATO DAI RAPPRESENTANTI DEI GRUPPI**

*Mercoledì 8 maggio 2024.*

L'ufficio di presidenza si è riunito dalle 12.50 alle 12.55.

**AUDIZIONI INFORMALI**

*Mercoledì 8 maggio 2024.*

**Audizione informale del Dirigente superiore, Direttore del Servizio Polizia Postale e Telecomunicazioni, dott. Ivano Gabrielli, nell'ambito dell'esame, ai fini della verifica della conformità al principio di sussidiarietà, della proposta di direttiva del Parlamento europeo e del Consiglio relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e il materiale pedopornografico, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (rifusione) (COM(2024)60 final).**

L'audizione informale è stata svolta dalle 14 alle 14.50.

**INDAGINE CONOSCITIVA**

*Mercoledì 8 maggio 2024. — Presidenza del presidente Alessandro GIGLIO VIGNA. — Interviene il Ministro per gli Affari europei il Sud, e le politiche di coesione e il PNRR Raffaele Fitto.*

**La seduta comincia alle 15.05.**

**Indagine conoscitiva sull'efficacia dei processi d'attuazione delle politiche dell'Unione europea e di utilizzo dei fondi strutturali e d'investimento europei per il Sistema-Paese.**

**Audizione del Ministro per gli affari europei, le politiche di coesione e il Piano nazionale di ripresa e resilienza, Raffaele Fitto.**

*(Svolgimento e conclusione).*

Alessandro GIGLIO VIGNA, *presidente*, avverte che la pubblicità dei lavori della seduta odierna sarà assicurata anche mediante la resocontazione stenografica e attraverso la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Il Ministro Raffaele FITTO svolge una relazione sui temi oggetto dell'audizione.

Intervengono, per formulare quesiti ed osservazioni, i deputati Stefano CANDIANI (LEGA), Piero DE LUCA (PD-IDP), Antonio GIORDANO (FDI), Alessandro GIGLIO VIGNA (LEGA), *presidente*.

Il Ministro Raffaele FITTO risponde ai quesiti posti e fornisce ulteriori precisazioni.

Alessandro GIGLIO VIGNA, *presidente*, ringrazia il Ministro per il suo intervento.

Dichiara quindi conclusa l'audizione.

**La seduta termina alle 16.15.**

---

*N.B.: Il resoconto stenografico della seduta è pubblicato in un fascicolo a parte.*

ALLEGATO

**Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. C. 1717 Governo.**

**PARERE APPROVATO DALLA COMMISSIONE**

La XIV Commissione Politiche dell'Unione europea,

esaminato, per i profili di competenza, il disegno di legge in titolo, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (C. 1717 Governo);

considerato che il quadro geopolitico attuale, caratterizzato da gravi conflitti internazionali tuttora in corso, pone in primo piano il rischio di crescenti minacce informatiche e richiede pertanto l'introduzione di misure volte ad una più efficace gestione e mitigazione dei suddetti rischi;

rilevata la necessità di prevenire le minacce alla sicurezza informatica attraverso modifiche sostanziali e processuali in relazione ai reati informatici, anche tramite il rafforzamento delle funzioni dell'Agenzia per la cybersicurezza nazionale (ACN) e il suo coordinamento con l'Autorità giudiziaria in caso di attacchi informatici;

evidenziato che il provvedimento è finalizzato a rispondere alla crescente offensività delle aggressioni realizzate con mezzi telematici ed informatici e alla conseguente esigenza di realizzare una più intensa tutela della sicurezza cibernetica;

sottolineato, in particolare, che il Capo I del disegno di legge contiene disposizioni concernenti la cybersicurezza nazionale finalizzate a conseguire una più elevata capacità di protezione e risposta di fronte a emergenze cibernetiche mentre il Capo II reca disposizioni per la prevenzione e il contrasto dei reati informatici, nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici;

ricordato che la materia della sicurezza cibernetica è regolata a livello dell'Unione europea dalla direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. direttiva NIS – *Network and Information Security*) recepita nell'ordinamento interno con il decreto legislativo 18 maggio 2018, n. 65, che costituisce la cornice legislativa 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;

ricordato altresì che la legge di delegazione europea 2022-2023 (legge 21 febbraio 2024, n. 15) ha delegato il Governo a dare attuazione alla nuova direttiva (UE) 2022/2555 del 14 dicembre 2022 (c.d. direttiva NIS 2) che ha sostituito il quadro di riferimento in materia, al fine di tenere conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza;

ritenuto che l'intervento legislativo risponda in modo adeguato ed efficace alla complessità e rapidità degli scenari di crisi, rafforzando il ruolo istituzionale dell'ACN anche in relazione alle sfide dell'attuale contesto caratterizzato da nuove tipologie di confronto ibrido;

evidenziato che il disegno di legge non presenta profili d'incompatibilità con l'ordinamento dell'Unione europea,

esprime

PARERE FAVOREVOLE.