COMMISSIONI RIUNITE

I (Affari costituzionali, della Presidenza del Consiglio e interni) e II (Giustizia)

S O M M A R I O

SEDE REFERENTE

Mercoledì 13 marzo 2024. — Presidenza del presidente della I Commissione, Nazario PAGANO. — Intervengono il sottosegretario di Stato alla Presidenza del Consiglio dei ministri, Alfredo Mantovano, il Viceministro della giustizia, Francesco Paolo Sisto (in videoconferenza) e la sottosegretaria di Stato ai rapporti con il Parlamento, Matilde Siracusano.

La seduta comincia alle 13.35.

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

(Esame e rinvio).

Le Commissioni iniziano l'esame del provvedimento.

Nazario PAGANO, *presidente e relatore per la I Commissione*, a seguito della richiesta di attivazione dell'impianto audiovisivo a circuito chiuso, e non essendovi obiezioni, ne dispone l'attivazione.

Procede quindi, in qualità di relatore per la I Commissione, a svolgere l'intervento introduttivo, ricordando che il provvedimento all'esame delle Commissioni riunite è composto da 18 articoli, distribuiti in due Capi, recanti rispettivamente: disposizioni in materia di rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'agenzia per la cybersicurezza nazionale, nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici (articoli da 1 a 10) e 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 (articoli da 11 a 18).

Prima di procedere all'illustrazione dei contenuti del provvedimento, rammenta 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*) 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 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. Rammenta che la normativa europea è stata successivamente aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 (c.d. direttiva NIS 2), al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza e al fine di eliminare le ampie divergenze tra gli Stati membri con riguardo agli obblighi in materia di sicurezza e segnalazione degli incidenti, nonché in materia di vigilanza ed esecuzione. La delega per la trasposizione della direttiva nel diritto interno è contenuta nella legge di delegazione europea 2022-2023 (legge 21 febbraio 2024, n. 15). Successivamente alla attuazione della NIS 1, il decreto-legge 21 settembre 2019, n. 105, è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica (PNSC) e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi. Con il decreto-legge 14 giugno 2021, n. 82, si è proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale, in attuazione di precisi obiettivi del Piano nazionale di ripresa e resilienza (PNRR): la sicurezza cibernetica costituisce, infatti, uno dei principali interventi previsti dal PNRR nell'ambito della trasformazione digitale della pubblica amministrazione e della digitalizzazione del Paese.

Nell'accingersi ad illustrare i contenuti del provvedimento, fa presente che nella sua relazione si dedicherà agli articoli relativi al Capo I, di competenza della I Commissione, rinviando alla relazione dell'onorevole Maschio per quanto riguarda il contenuto del Capo II.

Segnala pertanto che l'articolo 1, al comma 1, prevede un obbligo di segnalazione di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici in carico ai seguenti soggetti: pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni previsto dall'articolo 1, comma 3, della legge di contabilità e finanza pubblica (legge n. 196 del 2009); regioni e province autonome di Trento e di Bolzano; comuni con popolazione superiore a 100.000 abitanti e comunque i comuni capoluoghi di regione; società di trasporto pubblico con bacino di utenza non inferiore a 100.000 abitanti; aziende sanitarie locali; società *in house* degli enti fin qui richiamati. Il comma 2 indica le modalità con le quali effettuare la notifica: una prima segnalazione deve avvenire senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza; entro settantadue ore dal medesimo momento dovrà avvenire la notifica completa di tutti gli elementi informativi disponibili. I commi 4 e 5 indicano le sanzioni per la violazione dell'obbligo di notifica. In particolare, il comma 4 prevede, in caso di inosservanza, la comunicazione da parte dell'Agenzia per la cybersicurezza nazionale all'interessato che la reiterazione dell'inosservanza comporterà l'applicazione delle sanzioni previste dal successivo comma 5. In caso di inosservanza l'Agenzia inoltre può disporre ispezioni, anche al fine di verificare l'attuazione da parte dei soggetti interessati di interventi di rafforzamento della loro resilienza rispetto al rischio di incidenti, interventi direttamente indicati dall'Agenzia ovvero previsti da apposite linee guida adottate dall'Agenzia. Il comma 5 individua la sanzione amministrativa pecuniaria per la reiterata inosservanza dell'obbligo di notifica da un minimo di 25.000 a un massimo di 125.000 euro. In base al comma 3, i soggetti indicati al comma 1 possono anche effettuare notifiche volontarie di incidenti ulteriori rispetto a quelli oggetto di obbligo di notifica. Il comma 6 esclude alcuni specifici soggetti dall'ambito di applicazione dell'articolo.

Passando a descrivere i contenuti dell'articolo 2, evidenzia che esso interviene in materia di mancato o ritardato adegua-

mento a segnalazioni dell'Agenzia per la cybersicurezza nazionale. In particolare, il comma 1 prevede che l'Agenzia per la cybersicurezza nazionale (ACN) possa segnalare, ad una serie di soggetti pubblici o che forniscono servizi pubblici, specifiche vulnerabilità cui essi risultano potenzialmente esposti; inoltre prevede che i destinatari di tali segnalazioni devono provvedere senza ritardo, e comunque non oltre 15 giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia. Il comma 2 prevede l'applicazione di una sanzione amministrativa pecuniaria in caso di mancata o ritardata adozione degli interventi risolutivi indicati dall'ACN. Si tratta della medesima sanzione per la reiterata inosservanza dell'obbligo di notifica all'ACN degli incidenti cibernetici indicata all'articolo 1, comma 5, del provvedimento in esame. La sanzione è comminata dall'ACN. La sanzione non si applica nel caso in cui motivate esigenze di natura tecnico-organizzativa, che devono essere tempestivamente comunicate all'Agenzia per la cybersicurezza nazionale, ne impediscano l'adozione o ne comportino il differimento oltre il termine di 15 giorni.

Quanto all'articolo 3, sottolinea che la disposizione interviene sull'articolo 1 del decreto-legge n. 105 del 2019 (c.d. decreto perimetro), inserendo due modifiche al comma 3-*bis*, che ha incrementato gli obblighi di notifica posti in capo ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica. In base alla lettera *a)* del comma 1, gli obblighi di notifica già previsti per gli incidenti aventi impatto su beni destinati a essere impiegati nel perimetro di sicurezza nazionale cibernetica (« beni ICT ») sono estesi anche agli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del perimetro, ma che sono di pertinenza di soggetti inclusi nel perimetro. In ragione della modifica introdotta i soggetti inclusi nel Perimetro devono effettuare la segnalazione di tali incidenti, senza ritardo e comunque al massimo entro 24 ore, nonché, come già previsto, devono provvedere alla notifica entro 72 ore. Con la seconda modifica, di cui alla lettera *b)* del comma 1, si prevede l'applicazione di una sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 per i casi di reiterata inosservanza dell'obbligo di notifica. Segnala che le modifiche introdotte dall'articolo 3 sono finalizzate, come evidenziato anche nella relazione illustrativa, al raccordo e al coordinamento delle disposizioni del citato decreto-legge n. 105 del 2019 con quelle recate dal provvedimento in esame, segnatamente all'articolo 1.

Rileva poi che 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. A tal fine, l'unico comma dell'articolo 4 interviene sull'articolo 8 del decreto-legge 14 giugno 2021, n. 82, che ha costituito il Nucleo per la cybersicurezza, prevedendo che il Nucleo possa essere convocato per formulare proposte di iniziative in materia di cybersicurezza nella composizione ristretta – e, dunque, con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati –, di volta in volta estesa alla partecipazione di specifici soggetti, tra i quali un rappresentante della Direzione nazionale antimafia e antiterrorismo o della Banca d'Italia.

Fa presente poi che l'articolo 5 reca disposizioni in materia di coordinamento operativo tra i servizi di informazione per la sicurezza e l'Agenzia per la cybersicurezza nazionale. Nel dettaglio, il comma 1 prevede che i servizi di sicurezza della Repubblica informino – per il tramite del Dipartimento delle informazioni per la sicurezza – il Presidente del Consiglio dei ministri o l'Autorità delegata per la sicurezza della Repubblica, ove istituita, nel caso in cui, avuta notizia di un evento o di un incidente informatico, ritengano strettamente necessario, per il perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza della Repubblica, il differimento di una o più attività di resilienza di competenza dell'Agenzia per

la cybersicurezza nazionale. Il comma 2 dispone che, in tali casi, il Presidente del Consiglio dei ministri, sentiti il direttore generale del Dipartimento delle informazioni per la sicurezza e il direttore generale dell'Agenzia per la cybersicurezza nazionale, può disporre il differimento degli obblighi informativi cui è in ogni caso tenuta la citata Agenzia, nonché il differimento di una o più delle sopra citate attività di resilienza.

Passando a descrivere i contenuti dell'articolo 6, fa presente che la disposizione istituisce, per le pubbliche amministrazioni indicate nell'articolo 1, comma 1, dove non sia già presente, la struttura preposta alle attività di cybersicurezza; al contempo, predispone l'istituzione del referente per la cybersicurezza, unico punto di contatto delle amministrazioni coinvolte con l'Agenzia per la cybersicurezza nazionale. Precisa, infine, quali soggetti e quali organi dello Stato siano esclusi dall'applicazione dei nuovi obblighi e per cui permane la disciplina precedente. Più nel dettaglio, il comma 1 individua, primariamente, i soggetti delle pubbliche amministrazioni coinvolti. Si tratta delle pubbliche amministrazioni trattate nell'articolo 1, comma 1, del disegno di legge salvo non presentino già la struttura costituenda. Tali soggetti, qualora non la possiedano ancora, devono dotarsi di una struttura per la cybersicurezza, anche fra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente. Le lettere da *a)* a *g)* del comma 1 individuano i compiti demandati a tale struttura: dallo sviluppo di politiche e procedure di sicurezza delle informazioni alla predisposizione di un piano per il rischio informatico; dall'elaborazione di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione ad interventi di potenziamento delle capacità di gestione dei rischi informatici; dall'attuazione delle misure previste dalle linee guida emanate dall'Agenzia per la cybersicurezza nazionale al monitoraggio delle minacce alla sicurezza. Il comma 2 istituisce la figura del referente per la cybersicurezza all'interno delle strutture appena descritte nel comma 1. Il referente, il cui nominativo dovrà essere prontamente comunicato all'Agenzia per la cybersicurezza nazionale, dovrà essere individuato in ragione delle qualità professionali possedute e opererà come punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale. Il comma 3 individua i soggetti e gli organi dello Stato a cui non si applicano le disposizioni presenti. In particolare, la lettera *a)* specifica l'esclusione delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati, elencati dal decreto del Presidente del Consiglio dei Ministri n. 131 del 31 luglio 2020 (si tratta dei soggetti già inclusi nel perimetro di sicurezza nazionale cibernetica e per i quali già risultano in vigore specifici obblighi di sicurezza), mentre la lettera *b)* specifica l'esclusione per quegli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza.

Evidenzia che l'articolo 7 inserisce tra le funzioni dell'Agenzia per la cybersicurezza nazionale (ACN) la valorizzazione dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale. A tal fine, il disegno di legge modifica il decreto-legge n. 82 del 2021, che ha definito l'architettura della cybersicurezza nazionale e ha istituito e disciplinato l'ACN, ed in particolare il comma 1 dell'articolo 7 che individua puntualmente le funzioni dell'agenzia. Attraverso l'inserimento della nuova lettera *m-quater*), tra le funzioni istituzionali dell'ACN viene ricompresa quella della promozione e sviluppo di ogni iniziativa, anche di partenariato tra soggetti pubblici e privati, per la valorizzazione dell'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale; ciò anche al fine di favorire un uso etico e corretto dei sistemi basati sulla IA.

Fa presente che l'articolo 8 definisce tempi e modalità per l'adozione del regolamento che dovrà stabilire termini e modalità per l'accertamento, la contestazione e la notificazione delle violazioni della nor-

mativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia. Più in particolare, introducendo un nuovo comma 4-*quater* all'articolo 17 del decreto-legge n. 82 del 2021, l'articolo 8 prevede che la disciplina del procedimento sanzionatorio amministrativo dell'Agenzia per la cybersicurezza nazionale sia definita con regolamento adottato entro 90 giorni con decreto del Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la cybersicurezza, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400. Il regolamento dovrà definire i termini e le modalità per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni che sono di competenza dell'Agenzia. La disposizione stabilisce infine che nelle more dell'entrata in vigore di tale regolamento, ai procedimenti sanzionatori si applicano le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689.

Evidenzia che il successivo articolo 9, introducendo il nuovo comma 8-*ter* all'articolo 12 del decreto-legge n. 82 del 2021, 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 per la cybersicurezza nazionale che abbiano partecipato, nell'interesse e a spese dell'Agenzia stessa, a specifici percorsi formativi di specializzazione. Tale divieto non si applica al personale che sia cessato dal servizio presso l'Agenzia in caso di collocamento a riposo d'ufficio al raggiungimento del requisito anagrafico previsto dalla legge per la pensione di vecchiaia; cessazione a domanda per inabilità; dispensa dal servizio dovuta a motivi di salute.

Sottolinea infine che l'articolo 10 introduce alcuni criteri di cybersicurezza nella disciplina dei contratti pubblici. In dettaglio, il comma 1 prevede l'adozione di un decreto del Presidente del Consiglio dei ministri, entro 120 giorni dalla data di entrata in vigore del provvedimento in esame, su proposta dell'Agenzia per la cybersicurezza nazionale e previo parere del Comitato interministeriale per la cybersicurezza (CIC), per individuare 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 alla tutela degli interessi nazionali strategici. La disposizione precisa che per elementi essenziali di cybersicurezza si intende « l'insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela » degli interessi nazionali strategici. Tale regolamentazione troverà applicazione per le pubbliche amministrazioni, i gestori di servizi pubblici e le società a controllo pubblico, ma anche – in base al comma 3 – per gli altri soggetti privati rientranti nel perimetro di sicurezza nazionale cibernetica (PSNC) di cui all'articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019. Si tratta dei soggetti aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Il comma 2 prevede, nell'ambito dei contratti di approvvigionamento di beni e servizi informatici di cui al comma 1, una serie di obblighi e facoltà in capo alle stazioni appaltanti, incluse le centrali di committenza, in relazione agli elementi essenziali di cybersicurezza individuati dal comma precedente. Nel dettaglio viene previsto che le stazioni appaltanti, incluse le centrali di committenza: possono esercitare la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici (di cui al decreto legislativo n. 36 del 2023), se accertano che l'offerta non tiene in considerazione gli elementi essenziali di cybersicurezza; considerano sempre gli elementi essenziali di cybersicurezza

nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione; nel caso in cui sia utilizzato il criterio del minor prezzo, inseriscono gli elementi di cybersicurezza di cui al comma 1 tra i requisiti minimi dell'offerta; nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliscono un tetto massimo per il punteggio economico entro il limite del 10%. Rileva che le disposizioni introdotte dall'articolo in esame si inseriscono in un sistema normativo di approvvigionamento di beni ICT disciplinato principalmente dall'articolo 1 del decreto-legge n. 105 del 2019, che il comma 4 fa espressamente salvo. Passa quindi la parola al presidente Maschio per l'illustrazione del Capo II del provvedimento.

Ciro MASCHIO, *presidente e relatore per la II Commissione*, prima di procedere ad illustrare le disposizioni di maggior interesse della Commissione Giustizia (Capo II, articoli da 11 a 18), richiama l'attenzione dei colleghi sulla delicatezza della materia oggetto del provvedimento, che si propone di colmare le lacune che inevitabilmente si vengono a creare nella legislazione volta a tutelare la sicurezza nazionale, delle pubbliche amministrazioni, delle imprese e dei cittadini a seguito dell'impetuoso sviluppo di tecnologie potenzialmente aggressive.

Sottolinea quindi come vi sia certamente una piena consapevolezza sulla necessità condivisa che il legislatore intervenga per adeguare la normativa sul tema.

Ciò premesso, con riguardo al contenuto dei restanti articoli del provvedimento, segnala che l'articolo 11 contiene modifiche al codice penale. In particolare, la lettera *a)* interviene sull'articolo 615-*ter* (accesso abusivo ad un sistema informatico o telematico). Per le ipotesi aggravate previste al secondo comma, in primo luogo sono raddoppiati i limiti edittali minimi e massimi della reclusione (da due a dieci anni). Inoltre, al medesimo comma l'aggravante di cui al numero 2) è integrata nel senso di affiancare all'uso della violenza anche l'impiego della minaccia e quella di cui al numero 3) è ampliata al fine di comprendervi altresì l'ipotesi in cui dal fatto derivi « la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare » dei dati, di informazioni o programmi contenuti nel sistema informativo.

Con riguardo all'ulteriore aggravante del terzo comma – riferita ad una condotta che riguardi sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico – evidenzia che la pena della reclusione è aumentata da 3 a 10 anni ovvero da 4 a 12 anni nella fattispecie pluriaggravata. Inoltre, qualora concorra l'aggravante numero 3) del secondo comma e quella del terzo comma, è previsto il divieto di equivalenza o prevalenza delle attenuanti (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo previste dall'introducendo articolo 623-*quater*) e che le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.

In riferimento al divieto di prevalenza delle attenuanti sulle aggravanti, che nel testo ricorre frequentemente, ricorda che la Corte costituzionale con la sentenza n. 197 del 2023 nel dichiarare l'illegittimità costituzionale dell'articolo 577, terzo comma, del codice penale che prevedeva un siffatto divieto ha comunque affermato che al legislatore – nell'esercizio della propria discrezionalità – è certamente consentito derogare al regime del bilanciamento purché la medesima deroga sia conforme ai principi costituzionali.

Fa quindi presente che la lettera *b)* interviene sull'articolo 615-*quater* del codice penale (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici). La disposizione modifica, in primo luogo, la definizione della fattispecie delittuosa, ampliando il dolo specifico previsto per la configurabilità della fattispecie sostituendo la parola « profitto » con « vantaggio ». Resta inalterato il si-

stema delle aggravanti, sostituendosi – secondo quanto riportato dalla relazione illustrativa – l'improprio rinvio all'articolo 617-*quater*, quarto comma, con il richiamo alle corrispondenti aggravanti di cui all'articolo 615-*ter* e, contestualmente, distribuendole in due commi e irrobustendo le relative cornici edittali. Evidenzia che la prima aggravante – assistita dalla pena della reclusione da 2 a 6 anni – concerne l'ipotesi in cui il fatto è commesso da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da parte di un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema. La seconda aggravante – punita con la reclusione da 3 a 8 anni – riguarda l'ipotesi in cui il fatto è commesso su sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

La lettera *c)* abroga l'articolo 615-*quinquies* del codice penale, il cui contenuto è però integralmente riprodotto dal nuovo articolo 635-*quater*.1, introdotto dalla lettera *p)*, cui si rinvia. Segnala quindi che la lettera *d)* interviene sull'articolo 617-*bis* del codice penale (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche e telefoniche). Anche in tal caso, si richiama la circostanza aggravante a effetto speciale, con l'applicazione della reclusione da 2 a 6 anni, qualora ricorra l'aggravante numero 1) dell'articolo 615-*ter*, secondo comma. Tale circostanza aggravante assorbe pertanto parzialmente la fattispecie prevista dal vigente secondo comma (terzo comma a seguito delle modifiche introdotte dalla disposizione in commento), che viene conseguentemente modificato al fine di coordinare le due disposizioni.

Fa presente che la lettera *e)* interviene sull'articolo 617-*quater* del codice penale (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche). La disposizione in commento reca alcune modifiche in materia di aggravanti, concernenti l'innalzamento della pena della reclusione da 4 a 10 anni (anziché da 3 a 8 anni) per le fattispecie aggravate, la previsione dell'aggravante della commissione del fatto su sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la previsione dell'aggravante della commissione del fatto in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni. Anche in tale sede si introduce il divieto di equivalenza o prevalenza delle attenuanti (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo, previste dall'introducendo articolo 623-*quater*) sull'aggravante della commissione del fatto su sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, prevedendo che le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.

La lettera *f)* interviene sull'articolo 617-*quinquies* del codice penale (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche). Segnala che la disposizione reca modifiche alla disciplina delle aggravanti, innalzando le pene e ridefinendo le fattispecie, analogamente a quanto previsto dalla lettera *e)* per l'articolo 617-*quater*. In particolare, si prevede l'aggravante, con applicazione della reclusione da 2 a 6 anni, della commissione del fatto in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni. Ancora, si prevede l'aggravante, con applicazione della reclusione da 3 a 8 anni, della commissione del fatto su sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico. Infine, si introduce anche in questo caso il divieto di equivalenza o prevalenza delle attenuanti (diverse dal vizio parziale di

mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo, previste dall'introducendo articolo 623-*quater*) sull'aggravante della commissione del fatto su sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, prevedendo che le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.

Segnala che la lettera *g)* interviene sull'articolo 617-*sexies* del codice penale (Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche). La disposizione in commento prevede l'innalzamento della pena della reclusione da 3 a 8 anni (anziché da 1 a 5 anni) per la fattispecie aggravata e la contestuale ridefinizione della medesima fattispecie aggravata, richiamando l'articolo 617-*quater* come novellato dalla lettera *e)* del testo in esame. Infine, si introduce anche in questo caso il divieto di equivalenza o prevalenza delle attenuanti (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo, previste dall'introducendo 623-*quater*) sull'aggravante della commissione del fatto su sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, prevedendo che le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.

La lettera *h)* reca una disposizione di coordinamento volta a modificare la rubrica del capo III-bis del titolo XII del libro secondo del codice penale, ora denominato « Disposizioni comuni », conseguentemente all'introduzione dell'articolo 623-*quater*.

Fa quindi presente che la lettera *i)* prevede l'inserimento dell'articolo 623-*quater* del codice penale (Circostanze attenuanti) con riguardo ai delitti oggetto di intervento del presente provvedimento (« reati informatici »). In primo luogo, viene introdotta una circostanza attenuante a effetto comune (diminuzione della pena fino a un terzo) quando il fatto sia di lieve entità, avuto riguardo alla natura, alla specie, ai mezzi, alle modalità o alle circostanze dell'azione o alla particolare tenuità del danno o del pericolo. Inoltre, si introduce una circostanza attenuante a effetto speciale (diminuzione della pena dalla metà a due terzi quando) in favore di chi si adopera per evitare che l'attività delittuosa sia portata a ulteriori conseguenze, anche aiutando concretamente l'autorità giudiziaria o l'autorità di polizia nella raccolta di prove o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi. Alle predette attenuanti non si applica il divieto di prevalenza sancito dall'articolo 69, quarto comma, del codice penale.

La lettera *l)* integra l'articolo 629 del codice penale (Estorsione) al fine di punire la fattispecie del delitto di estorsione mediante reati informatici, realizzata dalla costrizione di taluno a fare o ad omettere qualche cosa, procurando a sé o ad altro un ingiusto profitto, mediante le condotte, o la minaccia di compierle, di cui ai reati ivi richiamati. Si prevede che la nuova fattispecie delittuosa sia punita con la reclusione da 6 a 12 anni e con la multa da euro 5.000 a euro 10.000, mentre si prevede la reclusione da 8 a 22 anni e la multa da euro 6.000 a euro 18.000 se ricorre taluna delle circostanze « indicate nell'ultimo capoverso dell'articolo precedente ». Il riferimento è all'articolo 628 del codice penale (rapina) e va presumibilmente interpretato come un rinvio al vigente terzo comma dell'articolo 628, in considerazione del fatto che l'identico rinvio contenuto nel secondo comma dell'articolo 629 è stato costantemente interpretato dalla giurisprudenza, anche dopo l'aggiunta di commi successivi, come riferito al terzo comma dell'articolo 628, che enumera le circostanze aggravanti del delitto di rapina.

Segnala che la lettera *m)* interviene sull'articolo 635-*bis* del codice penale (Danneggiamento di informazioni, dati e programmi informatici). La disposizione prevede in primo luogo l'innalzamento della pena della reclusione da 2 a 6 anni (anzi-

ché da 6 mesi a 3 anni) per la fattispecie semplice. Inoltre si amplia la fattispecie aggravata, prevedendo che essa ricorra se il fatto è commesso da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo (oltre che con abuso della qualità di operatore di sistema, come già previsto dal testo vigente). Ancora, essa ricorre in caso di uso di violenza o minaccia o in caso di persona palesemente armata (rispetto al testo vigente l'aggravante è estesa pertanto alle ipotesi della violenza alle cose e della persona palesemente armata). Per la fattispecie aggravata la pena è la reclusione da 3 a 8 anni (anziché da 1 a 4 anni).

Segnala che la lettera *n)* interviene sull'articolo 635-*ter* del codice penale (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità). La disposizione interviene, in primo luogo, sulla definizione della fattispecie, prevedendo che i fatti descritti debbano essere diretti a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico. Tale definizione, sostituisce quella della commissione del fatto in danno di un sistema utilizzato dallo Stato o da enti pubblici o da imprese esercenti servizi pubblici prevista dal testo vigente. Viene conseguentemente modificata anche la rubrica dell'articolo. Si ridefiniscono quindi le circostanze aggravanti, con l'applicazione della pena della reclusione da 3 a 8 anni. La prima circostanza aggravante opera se il fatto è commesso da un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema (il testo vigente fa riferimento solo all'abuso della qualità di operatore di sistema e prevede l'aumento della pena fino a un terzo). La seconda opera nel caso di uso di violenza o minaccia o se il fatto è commesso da persona palesemente armata (rispetto al testo vigente l'aggravante è estesa pertanto alle ipotesi della violenza alle cose e della persona palesemente armata ed è inasprito il trattamento sanzionatorio, prevedendo il testo vigente l'aumento della pena fino a un terzo). La terza circostanza aggravante riguarda la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi (rispetto al testo vigente, l'aggravante è estesa alle ipotesi di sottrazione o inaccessibilità dei dati o dei programmi). Infine, la norma prevede, nel caso di concorso delle prime due circostanze aggravanti con la terza, la pena della reclusione da 4 a 12 anni e il divieto di equivalenza o prevalenza delle attenuanti (diverse dal vizio parziale di mente, dalla minore età nonché da quelle della lieve entità e del recesso attivo, su cui vedi infra, previste dall'introducendo articolo 623-*quater*).

Fa presente che la lettera *o)* interviene sull'articolo 635-*quater* del codice penale (Danneggiamento di sistemi informatici o telematici). La disposizione prevede, con modifiche analoghe a quelle proposte per l'articolo 635-*bis*, in primo luogo l'innalzamento della pena della reclusione da 2 a 6 anni (anziché da 1 a 5 anni) per la fattispecie semplice. In secondo luogo si ampia anche in questo caso la fattispecie aggravata, prevedendo che essa ricorra se il fatto è commesso da parte di un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo (oltre che con abuso della qualità di operatore di sistema, come già previsto dal testo vigente), ovvero usando violenza o minaccia o da parte di persona palesemente armata (rispetto al testo vigente l'aggravante è estesa pertanto alle ipotesi della violenza alle cose e della persona palesemente armata). Per tale fattispecie aggravata la pena è aumentata, prevedendosi la reclusione da 3 a 8 anni; le circostanze aggravanti sono pertanto configurate quali a effetto speciale, anziché a effetto comune, come invece previsto dal testo vigente.

Evidenzia quindi che la lettera *p)* introduce l'articolo 635-*quater*.1 del codice penale (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico). In realtà il primo comma del nuovo articolo riproduce il vigente articolo 615-*quinquies* (che viene contestualmente abrogato dalla lettera *c)* dell'articolo in commento. I successivi due commi prevedono invece nuove circostanze aggravanti, che ricorrono se il fatto è commesso da un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema (reclusione da 2 a 6 anni), oppure se il fatto riguarda sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico (reclusione da 3 a 8 anni).

La lettera *q)* novella l'articolo 635-*quinquies* del codice penale (Danneggiamento di sistemi informatici o telematici di pubblica utilità), sostituendo nella rubrica e nel testo le parole « pubblica utilità » con « pubblico interesse » e innalzando la pena della reclusione da due a sei anni (attualmente la pena prevista è da uno a quattro anni). Il secondo comma disciplina le circostanze aggravanti, con l'applicazione della pena della reclusione da 3 a 8 anni. La prima circostanza aggravante opera se il fatto è commesso da un pubblico ufficiale o incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema (il testo vigente fa riferimento solo all'abuso della qualità di operatore di sistema e prevede l'aumento della pena fino a un terzo). La seconda riguarda l'uso di violenza o minaccia o la commissione del fatto da parte di persona palesemente armata (rispetto al testo vigente l'aggravante è estesa pertanto alle ipotesi della violenza alle cose e della persona palesemente armata ed è inasprito il trattamento sanzionatorio, prevedendo il testo vigente l'aumento della pena fino a un terzo). La terza circostanza aggravante ricorre in caso di distruzione, deterioramento, cancellazione, alterazione o soppressione delle informazioni dei dati o dei programmi (il testo vigente prevede l'aggravante nel caso di distruzione, danneggiamento o inservibilità del sistema). Il terzo comma prevede, nel caso di concorso di taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma e di taluna delle circostanze di cui al n. 3 la pena della reclusione da 4 a 12 anni e il divieto di equivalenza o prevalenza delle attenuanti salve quelle dell'articolo 639-*ter* come proposto dal testo in esame alla lettera *r)* dell'articolo 11.

Tale lettera inserisce infatti l'articolo 639-*ter* del codice penale (circostanze attenuanti) per questa tipologia di reati. In particolare, è prevista una circostanza attenuante a effetto comune quando il fatto sia di lieve entità, avuto riguardo alla natura, alla specie, ai mezzi, alle modalità o alle circostanze dell'azione o alla particolare tenuità del danno o del pericolo. È altresì prevista un'attenuante a effetto speciale in favore di chi si adopera per evitare che l'attività delittuosa sia portata a ulteriori conseguenze, anche aiutando concretamente l'autorità giudiziaria o l'autorità di polizia nella raccolta di prove o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi. Alle predette attenuanti non si applica il divieto di prevalenza sancito dall'articolo 69, quarto comma, del codice penale.

Segnala che l'articolo 12 del provvedimento in esame reca modifiche al codice di procedura penale finalizzate a recepire gli interventi in materia di prevenzione e contrasto dei reati informatici introdotte dall'articolo 11.

La lettera *a)* interviene sull'articolo 51 del codice di procedura penale (Uffici del pubblico ministero. Attribuzioni del procuratore della Repubblica distrettuale) che al comma 3-*quinquies*, reca il catalogo dei reati informatici attribuiti alla competenza del procuratore distrettuale. Oltre a sopprimere il riferimento all'abrogando arti-

colo 615-*quinquies* sono inseriti i riferimenti agli articoli 635-*quater*.1 e 635-*quinquies* del codice penale nonché al delitto relativo alla comunicazione di dati, informazioni o elementi di fatto falsi tese a ostacolare o condizionare la formazione e trasmissione dell'elenco delle reti, sistemi informatici e informativi da parte degli operatori compresi nel perimetro di sicurezza cibernetica, le procedure di affidamento delle forniture di strumenti destinati ai servizi e sistemi informatici, o le attività ispettive o di vigilanza su reti, sistemi informatici e servizi informatici (tale fattispecie è prevista dall'articolo 1, comma 11, del decreto-legge n. 105 del 2019).

Segnala che le lettere *b)* e *c)* estendono ai reati informatici le deroghe relative al regime ordinario di notifica dell'avviso della richiesta di proroga delle indagini preliminari e di fissazione dell'udienza in camera di consiglio da parte del giudice per le indagini preliminari in caso di mancato accoglimento dell'istanza, nonché il regime che amplia a due anni il termine per le indagini preliminari, qualora il fatto sia commesso in danno di sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

Fa presente che l'articolo 13 reca alcune modifiche alle norme sui collaboratori di giustizia, di cui al decreto-legge n. 8 del 1991.

La lettera *a)* estende le condizioni di applicabilità delle speciali misure di protezione per i collaboratori di giustizia anche nei confronti degli autori di gravi delitti informatici, in relazione ai quali al procuratore nazionale antimafia e antiterrorismo sono riconosciute funzioni di impulso nei confronti dei procuratori distrettuali (elencati all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale).

La lettera *b)* estende – anche per i reati informatici – la comunicazione al Procuratore nazionale antimafia e antiterrorismo della proposta di ammissione alle speciali misure di protezione in favore del collaboratore di giustizia.

La lettera *c)* estende la disciplina speciale dei benefici penitenziari riservati ai soggetti che collaborano con la giustizia anche agli autori dei reati informatici (elencati nel citato articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale).

Evidenzia che l'articolo 14 estende la disciplina delle intercettazioni prevista per i fatti di criminalità organizzata ai reati informatici rimessi al coordinamento del procuratore nazionale antimafia e antiterrorismo. In sintesi, in base a tale disciplina derogatoria l'autorizzazione all'intercettazione è soggetta a limiti meno stringenti, potendo essere concessa quando sussistono « sufficienti indizi » di reato (anziché gravi indizi) e quando è « necessaria per lo svolgimento delle indagini » (anziché assolutamente indispensabile). Nelle stesse ipotesi le intercettazioni ambientali sono consentite nel domicilio o altro luogo di dimora privata anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa. La relativa durata è di 40 giorni, prorogabile per periodi successivi di 20 giorni. Nei casi di urgenza, alla proroga provvede direttamente il pubblico ministero, con decreto che viene immediatamente comunicato al giudice per le indagini preliminari, il quale entro quarantotto ore decide sulla convalida.

L'articolo 15 interviene sul catalogo dei reati presupposto della responsabilità amministrativa degli enti, contemplato dall'articolo 24-*bis* del decreto legislativo n. 231 del 2001.

Il comma 1 prevede di inasprire la sanzione pecuniaria applicata all'ente che commette i delitti informatici (che passano da un arco edittale compreso tra cento e cinquecento quote, ad un arco compreso tra duecento e settecento quote). Si prevede inoltre di applicare all'ente la sanzione pecuniaria da trecento a ottocento quote in relazione alla commissione della nuova fattispecie di estorsione informatica (articolo 629, terzo comma, del codice penale) e le relative sanzioni interdittive. Con il comma 2 la sanzione pecuniaria legata alla condotta dell'articolo 635-*quater*.1 viene elevata da trecento a quattrocento quote.

Evidenzia che l'articolo 16 interviene sul procedimento di applicazione delle speciali misure di protezione per i testimoni di giustizia e per gli altri protetti, prevedendo 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*, del codice di procedura penale).

L'articolo 17 disciplina i rapporti tra l'Agenzia per la cybersicurezza nazionale (ACN), il procuratore nazionale antimafia e antiterrorismo, la polizia giudiziaria ed il pubblico ministero novellando la disciplina vigente (articolo 17 del decreto-legge n. 109 del 2021). In primo luogo, la lettera *a)* prevede che la trasmissione delle notifiche di incidente da parte del personale dell'Agenzia addetto al CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione debba essere immediata.

La lettera *b)* introduce quattro ulteriori commi nel citato articolo 17 del decreto-legge n. 109 del 2021. Il primo prevede che l'Agenzia deve informare senza ritardo il Procuratore nazionale antimafia e antiterrorismo nei casi in cui ha notizia di un attacco ai sistemi informatici o telematici, e, in ogni caso quando risultino interessati soggetti qualificati (soggetti rientranti nel Perimetro di sicurezza nazionale; operatori di servizi essenziali e dei fornitori di servizio digitale, imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico). Corrispondentemente, il PM – quando acquisisce la notizia dei gravi delitti informatici deve darne tempestiva informazione all'ACN assicurando anche il raccordo informativo con l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione. Il PM, in ogni caso, ricevuta la notizia di reato e, assunta la direzione delle indagini, è chiamato ad impartire le disposizioni necessarie ad assicurare che gli accertamenti urgenti si svolgano tenendo conto delle attività di ripristino svolte dall'Agenzia e può eventualmente disporre il differimento di una o più delle attività, con motivato provvedimento adottato senza ritardo, per evitare un grave pregiudizio per il corso delle indagini. Viene, infine, introdotta la facoltà per l'ACN, in caso di accertamenti tecnici irripetibili per i delitti di cui all'articolo 371-*bis*, comma 4-*bis*, del codice di procedura penale, di assistere al conferimento dell'incarico e partecipare agli accertamenti, anche quando si procede nelle forme dell'incidente probatorio.

Segnala infine che l'articolo 18 reca le disposizioni finanziare, recando la consueta clausola di invarianza degli oneri e disponendo che i proventi delle sanzioni di cui all'articolo 1, comma 5, confluiscono nelle entrate dell'Agenzia per la cybersicurezza nazionale.

Nazario PAGANO, *presidente*, chiede al Sottosegretario Mantovano se intende intervenire in questa seduta o si riserva di farlo successivamente.

Il Sottosegretario Alfredo MANTOVANO, dopo aver ringraziato i Presidenti delle Commissioni e i loro componenti, fa presente che la sua presenza alla seduta odierna non va intesa come sostitutiva della Sottosegretaria Siracusano, che parteciperà al prosieguo dell'esame del provvedimento, bensì come volta a sottolineare l'importanza cruciale del disegno di legge proposto dal Governo. Per farlo ritiene sufficiente svolgere una sintetica descrizione dell'attuale stato dell'arte partendo dal ricordare che nel 2023 l'Agenzia per la cybersicurezza – istituita dal Governo Draghi – ha trattato 1.411 eventi, circa 117 al mese, con un notevole incremento rispetto ai dati del 2022. Specifica che con la parola « evento » si intende un avvenimento che ha un impatto su almeno un soggetto nazionale, che comporta un *alert* e un successivo intervento di rimedio nei confronti dei soggetti colpiti.

Specifica che l'ultimo anno e mezzo è stato caratterizzato da una duplice tipologia di eventi: anzitutto da eventi cosiddetti DDoS, attacchi *web* che mirano a fare danni, materiali o di immagine, prevalen-

temente orchestrati da gruppi *cyber* di attivisti filorussi e, da ultimo, filopalestinesi, che intervengono con una certa sincronia rispetto alle relative prese di posizione delle istituzioni nazionali in merito alla guerra in Ucraina o alla situazione di Israele; quindi da eventi cosiddetti *ransom*, che rappresentano la versione informatica dell'estorsione, realizzata attraverso la sottrazione di informazioni sensibili, che colpisce piccole e medie aziende, aziende sanitarie locali, ma anche privati cittadini che, dinanzi al rischio di veder divulgati propri dati personali, preferiscono pagare quanto viene loro richiesto piuttosto che denunciare il reato. Evidenzia l'elevato livello di pericolosità di questi attacchi informatici, che sono in grado di fermare una linea ferroviaria come di bloccare una sala operatoria, e sottolinea come la pandemia abbia inciso notevolmente su questi fenomeni perché il notevole trasferimento di attività sul *web* non è stato accompagnato dalla messa in sicurezza dei dati che sul *web* venivano trasferiti.

Rileva che la normativa vigente risale a 20 anni fa, rimarcando come per il *web* quel lasso di tempo corrisponda a un'era geologica. Fa quindi presente, ad esempio, che quanto alle sanzioni penali, oggi è più conveniente introdursi nei dati di una ASL per acquisire migliaia di dati sanitari e chiedere in *bitcoin* una somma ingente per non diffonderli, oppure estrarre dati sensibili da una banca dati istituzionale, con gravi contraccolpi istituzionali – come dimostrano i recenti casi di cronaca – piuttosto che realizzare un furto in una singola abitazione. Sottolinea, inoltre, l'attuale assenza di un formale coordinamento, a fronte dei suddetti attacchi, tra la polizia giudiziaria, l'autorità giudiziaria e l'Agenzia per la cybersicurezza, facendo l'esempio del blocco della sala operatoria, a fronte del quale ci si può chiedere se sia meglio ripristinarla subito, alterando la scena del crimine e quindi rinunciando ad acquisire gli elementi per perseguire il reato, ovvero privilegiare il contrasto al *cybercrime*, lasciando bloccata la sala operatoria con tutte le conseguenze del caso.

Lamenta quindi una diffusa scarsa consapevolezza, anche a livello istituzionale, dell'importanza di dotarsi di adeguate misure di sicurezza, rammentando una vicenda occorsa pochi giorni dopo aver assunto l'incarico di Governo quando, a richiesta del direttore dell'Agenzia per la cybersicurezza, ha dovuto chiamare personalmente un Ministro per avvisarlo che era in corso un attacco ai sistemi del ministero, non riuscendo a contattare, di sabato pomeriggio, il responsabile cyber del ministero stesso. Ritiene la vicenda emblematica della convinzione – trasversale nel nostro Paese e non modificabile al cambio dei Governi – per la quale il sabato pomeriggio e nel fine settimana non si lavora, mentre purtroppo è proprio in quei giorni che si concentrano gli attacchi informatici, che richiedono una attenzione continuativa. Così descritto lo stato dell'arte, ricorda che il 2024 è l'anno che vede l'Italia alla presidenza del G7 e il tema della cybersicurezza e dell'intelligenza artificiale al centro di varie riunioni ministeriali oltre che della riunione dei Capi di Stato e di Governo di giugno.

Evidenzia quindi che il disegno di legge all'esame delle Commissioni prova a rispondere a queste esigenze di sicurezza e a incrementare, con procedure di *alert* e tempi certi, una maggiore consapevolezza del rischio *cyber*, a superare comportamenti ingenui e debolezze, ad adottare misure organizzative adeguate, a dotarsi di una *governance* centralizzata degli aspetti di sicurezza e a innalzare le pene. Per quanto riguarda in particolare le sanzioni penali aggiunge che non si tratta di un mero incremento sanzionatorio, pur necessario, ma anche della possibilità – attraverso l'innalzamento delle pene – di utilizzare specifici strumenti investigativi e di realizzare il coordinamento delle indagini assegnandone la competenza alle direzioni distrettuali, con il coordinamento della direzione nazionale antimafia e antiterrorismo.

In conclusione, dopo aver chiarito che il tema dell'intelligenza artificiale non è oggetto di questo disegno di legge – che avrà una disciplina autonoma, alla quale il Governo sta già lavorando, e per la quale

occorre attendere anche l'emanazione di una specifica normativa europea – dichiara che il testo del provvedimento non è blindato, ma aperto all'apporto parlamentare, nella convinzione che questa materia sia estranea a contrapposizioni ideologiche, avendo tutti l'esigenza di operare un adeguamento normativo per elevare i livelli di sicurezza. Fa presente che nel frattempo le varie strutture interessate dagli attacchi *cyber* lavorano, a legislazione vigente, con difficoltà e nonostante i limiti che il disegno di legge mira a ridurre. Auspica quindi che la trattazione parlamentare del provvedimento, pur approfondita, si svolga in tempi che consentano al Paese di dotarsi al più presto di strumenti più adeguati.

Nazario PAGANO, *presidente*, dando la parola all'onorevole Boschi, fa presente che numerosi colleghi hanno già chiesto di intervenire in discussione generale.

Maria Elena BOSCHI (IV-C-RE), prima di intervenire in discussione generale, intende porre una questione relativa all'ordine dei lavori. Nel ricordare che entrambe le Commissioni sono convocate a breve su altri provvedimenti, rileva che il tempo a disposizione per la discussione generale odierna del disegno di legge in materia di cybersicurezza è pressoché esaurito. Senza nulla togliere al Viceministro Sisto e alla Sottosegretaria Siracusano che seguiranno l'iter del provvedimento, ritiene che ai fini del confronto sia molto preziosa la presenza del Sottosegretario Mantovano che ha una delega specifica sulla materia. Chiede quindi se vi sia la disponibilità del Sottosegretario Mantovano a tornare a una prossima seduta, al fine di consentire che la discussione generale si svolga alla sua presenza e che dunque si possa svolgere un proficuo approfondimento del tema, che non rappresenta come già rilevato un terreno di contrapposizione ideologica.

Nazario PAGANO, *presidente*, considera opportuno l'intervento dell'onorevole Boschi, confermando che nella giornata odierna non vi è tempo sufficiente a svolgere la discussione generale sul provvedimento, tanto più che diversi colleghi hanno chiesto di intervenire. Nel preannunciare che il Sottosegretario Mantovano per le vie brevi si è appena dichiarato disponibile a tornare la prossima settimana, ritiene che in quell'occasione si potrà svolgere senza fretta un utile confronto. Nel ringraziare il Viceministro Sisto e la Sottosegretaria Siracusano che con la consueta competenza affiancheranno le Commissioni I e II nel corso dell'esame del provvedimento, rinvia il seguito dell'esame ad una prossima seduta.

La seduta termina alle 14.05.

UFFICIO DI PRESIDENZA INTEGRATO DAI RAPPRESENTANTI DEI GRUPPI

Mercoledì 13 marzo 2024.

L'ufficio di presidenza si è riunito dalle 14.10 alle 14.20.