XIV COMMISSIONE PERMANENTE

(Politiche dell'Unione europea)

S O M M A R I O

SEDE CONSULTIVA

Martedì 15 ottobre 2019. — Presidenza del presidente Sergio BATTELLI.

La seduta comincia alle 12.30.

DL 105/2019: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
C. 2100 Governo.
(Parere alle Commissioni I e IX).

(Esame e rinvio).

La Commissione inizia l'esame del provvedimento in oggetto.

Sergio BATTELLI, *presidente*, precisa che il decreto scade il 20 novembre e segnala che il provvedimento è inserito all'ordine del giorno dell'Assemblea a partire da lunedì 21 ottobre e che, pertanto, la Commissione dovrà rendere il parere entro la seduta già convocata per domani alle 14.

Quindi, in sostituzione della relatrice Marina Berlinghieri, impossibilitata ad essere presente alla seduta, riferisce – per i profili di competenza – sul decreto-legge in materia di sicurezza cibernetica, ai fini del parere da rendere alle Commissioni riunite I e IX, premettendo che lo « spazio cibernetico » rappresenta un nuovo dominio operativo di natura artificiale, trasversale agli altri quattro domini tradizionali (dominio terrestre, dominio aereo, dominio marittimo, dominio spaziale), nel quale gli esseri umani, e nel prossimo futuro verosimilmente anche le intelligenze artificiali, possono agire e interagire a distanza.

Sottolinea che si tratta di un dominio di importanza strategica per lo sviluppo economico, sociale e culturale dei diversi Paesi ma al contempo un nuovo « spazio virtuale » di competizione economica e geopolitica per l'ampiezza dei settori che ne sono coinvolti e che, grazie ai progressi delle tecnologie di comunicazione e l'impiego diffuso di dispositivi elettronici e di monitoraggio, si intrecciano quotidianamente nello spazio cibernetico miliardi di interconnessioni, si scambiano conoscenze a livello globale e viene raccolto un gigantesco numero di dati e di informazioni compresi quelli di natura personale e sensibile (cosiddetto *big data)*.

Osserva che la dimensione cibernetica è pertanto generata dalla ramificatissima rete di infrastrutture materiali di collegamento e di comunicazione che, attraverso la tecnologia informatica, mettono in contatto tra loro un crescente numero di

esseri umani e permettono loro di attivare e controllare da ubicazioni remote macchine e apparati in tutto il mondo.

Rileva che si tratta di un ecosistema complesso nel cui ambito gli esperti della materia sono soliti distinguere i seguenti tre livelli essenziali: il livello fisico infrastrutturale, rappresentato dalle macchine (le architetture delle reti, i *computer*, i router, eccetera); il livello logico informativo rappresentato dal volume dei dati gestiti dalle macchine (*database*, file, ma anche software gestiti dalle macchine); il livello sociale cognitivo, ovvero l'insieme delle relazioni umane e delle caratteristiche socio-cognitive che possono costituire le identità virtuali (l'indirizzo *e-mail*, il profilo nei social network, gli indirizzi IP delle macchine).

Osserva che questa nuova realtà porta all'umanità nuove opportunità ma anche inediti pericoli, come si è visto per esempio emergere nel recente passato in Estonia, negli Stati Uniti e altrove.

Ricorda che il Consiglio dei ministri, nella seduta del 19 settembre 2019, ha dunque approvato il decreto n. 105 del 2019 – che introduce disposizioni urgenti in materia di « perimetro » di sicurezza nazionale cibernetica – mirato ad 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 e la previsione di misure idonee a garantire i necessari *standard* di sicurezza volti a minimizzare i rischi consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione.

Segnala, in particolare, che il decreto fa riferimento ad amministrazioni pubbliche, nonché ad enti oppure operatori nazionali, pubblici e privati i cui sistemi informatici: sono necessari per l'esercizio di una funzione essenziale dello Stato; sono necessari per l'assolvimento di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato; il cui malfunzionamento, interruzione o uso improprio possono pregiudicare la sicurezza nazionale.

Rammenta che resta ferma, per gli organismi di informazione e sicurezza, la specifica disciplina di cui alla legge 3 agosto 2007, n. 124 (recante « Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto »).

Evidenzia che, una volta stabilito il perimetro, verranno definite le procedure con le quali i soggetti che ne fanno parte dovranno notificare gli eventuali incidenti « aventi impatto su reti, sistemi informativi e servizi informatici » e vengono stabilite le misure « volte a garantire elevati livelli di sicurezza ».

Segnala, in particolare, l'articolo 1, comma 3, demanda ad un decreto del Presidente del Consiglio dei ministri – da adottare entro dieci mesi dalla conversione del decreto-legge – la definizione di ulteriori dettagli applicativi, per cui rimando alla documentazione predisposta dal Servizio Studi per le Commissioni in sede referente.

Fa presente che il testo integra e adegua, inoltre, il quadro normativo in materia di esercizio dei poteri speciali da parte del Governo, con particolare riferimento a quanto previsto dal decreto-legge 15 marzo 2012, n. 21, in modo da coordinare l'attuazione del regolamento (UE) 2019/452, sul controllo degli investimenti esteri, e apprestare idonee misure di tutela di infrastrutture o tecnologie critiche ad oggi non ricadenti nel campo di applicazione del decreto-legge 15 marzo 2012, n. 21.

Aggiunge che le nuove norme, tra l'altro, attribuiscono al Presidente del Consiglio dei ministri, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi, il potere di eliminare, ove indispensabile e per il tempo strettamente necessario, lo specifico fattore di rischio o di mitigarlo, secondo un criterio di proporzionalità, disattivando totalmente o parzialmente, uno o più apparati o prodotti impiegati nelle reti e nei sistemi.

Nello specifico, evidenzia che il decreto-legge stabilisce in quattro mesi il termine per individuare le amministrazioni pubbliche, gli enti e gli operatori pubblici e privati che entreranno a far parte del cosiddetto perimetro cibernetico, a tutela della sicurezza di reti e servizi definiti « strategici ». Sempre in quattro mesi con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), con un rappresentante della Presidenza del Consiglio dei ministri, dovranno stabilirsi i criteri in base ai quali i soggetti predisporranno e aggiorneranno « con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici sensibili di rispettiva pertinenza, comprensivo della relativa architettura e componentistica », che verrà poi diffuso agli organismi di competenza. Entro dieci mesi dovranno essere definite le procedure secondo cui i soggetti che fanno capo al perimetro notifichino gli incidenti che hanno impatto su reti, sistemi e servizi. Sempre entro dieci mesi è prevista la definizione delle misure volte a garantire gli elevati livelli di sicurezza previsti per i soggetti identificati, relative alle politiche di sicurezza, alla struttura organizzativa e alla gestione del rischio e alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza, alla protezione fisica e logica e dei dati, all'integrità delle reti e dei sistemi informativi, alla gestione operativa, ivi compresa la continuità del servizio, al monitoraggio, test e controllo, alla formazione e consapevolezza, all'affidamento di forniture di beni, sistemi e servizi di *information and communication technology* (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale.

Sotto il più specifico punto di vista della Commissione, evidenzia che sul piano europeo da molti anni è stato acceso il faro su tali problematiche, sottolineando che uno tra i primi documenti normativi che hanno posto il problema della tutela dei diritti nello spazio cibernetico e del contrasto dei reati che vengono commessi avvalendosi degli strumenti offerti dalla tecnologia e dall'ambiente informatici deve essere individuato nella Convenzione del Consiglio d'Europa sul crimine cibernetico, fatta a Budapest il 23 novembre 2001 ed entrata in vigore il 1º luglio 2004. A tal proposito ricorda che la firma della Convenzione fu l'esito del lavoro di una commissione istituita dal Comitato dei ministri del Consiglio d'Europa nel 1997 (la quale, a sua volta, proseguì il tracciato già indicato dalle Raccomandazioni del medesimo Consiglio d'Europa del 1989 n. 9 e del 1995 n. 13); rammenta che essa è stata ratificata dall'Italia con la legge 18 marzo 2008, n. 48, la Convenzione sul crimine cibernetico è stata seguita dal Protocollo addizionale del 28 gennaio 2003 (entrato in vigore il 1º marzo 2006), inerente al contrasto dei crimini di matrice razzista e xenofoba commessi mediante strumenti informatici Segnala peraltro che tale Protocollo non è stato ancora ratificato dall'Italia.

Rileva che le considerazioni di sistema contenute nel preambolo della Convenzione di Budapest appaiono di particolare rilievo, sottolineandosi in esse la necessità di perseguire una politica comune in campo penale, finalizzata alla protezione della società contro la criminalità informatica, adottando misure legislative appropriate e sviluppando la cooperazione internazionale, nella consapevolezza dei profondi cambiamenti dipendenti dall'introduzione della tecnologia digitale, dalla convergenza e costante globalizzazione delle reti informatiche.

Fa presente che il preambolo premette altresì la preoccupazione per i rischi che le reti informatiche e le informazioni in formato elettronico possano anche essere utilizzate per commettere reati e che le prove connesse a tali reati possano essere conservate e trasferite tramite queste reti.

Osserva che la Convenzione è pertanto finalizzata ad offrire un deterrente per le condotte dirette contro la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati informatici,

così come per l'uso improprio di questi sistemi, reti ed informazioni, attraverso la tipizzazione penale dei comportamenti indicati nella medesima Convenzione.

Rileva altresì che la Convenzione, nondimeno, tiene presente la necessità di garantire un equo bilanciamento tra l'interesse per l'azione repressiva e il rispetto dei diritti umani fondamentali come previsto nella Convenzione europea dei diritti dell'uomo del 1950, la Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici e gli altri trattati applicabili sui diritti umani che riaffermano il diritto di ciascuno di avere opinioni senza condizionamenti, come anche il diritto alla libertà di espressione, incluso il diritto di cercare, ricevere, e trasmettere informazioni e idee di ogni tipo, senza limiti di frontiere, e il diritto al rispetto della *privacy*.

Evidenzia che le acquisizioni dell'ordinamento del Consiglio d'Europa sono rifluite anche nell'ambito dell'Unione europea: l'articolo 83, comma 1, del Trattato sul funzionamento dell'Unione europea (TFUE) infatti prevede che il Parlamento europeo e il Consiglio, deliberando mediante direttive secondo la procedura legislativa ordinaria, possono stabilire norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente gravi che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni. Ricorda che tali sfere di criminalità comprendono – oltre, tra gli altri, al traffico illecito di stupefacenti e di armi, al riciclaggio di denaro, alla corruzione, alla criminalità organizzata – la criminalità informatica.

Osserva che è in questo solco che s'inserisce la direttiva NIS, recepita con il decreto legislativo 18 maggio 2018, n. 65, (direttiva (UE) 2016/1148). Ricorda che con essa è stata ulteriormente definita la cornice legislativa relativa alla sicurezza delle reti e dei sistemi informativi con espressa individuazione dei soggetti competenti a dare attuazione agli obblighi previsti dalla richiamata direttiva.

Evidenzia, in particolare, che la direttiva NIS ha stabilito misure per uno *standard* comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione 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 ». Sottolinea che la direttiva rappresenta il primo provvedimento di carattere generale adottato in ambito europeo sul tema della sicurezza cibernetica e delinea le azioni in capo agli Stati membri volte a migliorare le capacità di sicurezza dei singoli Paesi dell'Unione europea. Fa presente che la direttiva si pone inoltre l'obiettivo di aumentare il livello di collaborazione nella prevenzione delle minacce cibernetiche e nell'implementazione di misure di risposta agli attacchi *cyber*. In tal senso, infine, rammenta che il decreto legislativo n. 65 del 2018 ha stabilito l'inclusione nella strategia nazionale di sicurezza cibernetica delle previsioni in materia di sicurezza delle reti e dei sistemi informativi rientranti nell'ambito di applicazione del decreto.

Nessuno chiedendo di intervenire, rinvia il seguito dell'esame del provvedimento in titolo ad altra seduta.

La seduta termina alle 12.40.