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 27 gennaio 2021. — Presidenza del presidente della I Commissione Giuseppe BRESCIA.

La seduta comincia alle 13.35.

Schema di decreto del Presidente del Consiglio dei ministri recante regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza.
Atto n. 240.

(Esame e rinvio).

Le Commissioni iniziano l'esame del provvedimento.

Giuseppe BRESCIA, *presidente*, avverte che, come specificato anche nelle convocazioni, alla luce di quanto stabilito dalla Giunta per il Regolamento nella riunione del 4 novembre scorso, i deputati possono partecipare all'odierna seduta in sede referente in videoconferenza, in quanto nella seduta odierna non sono previste votazioni sul provvedimento.

Segnala che le Commissioni riunite I e IX avviano oggi l'esame, in sede atti del Governo, dello Schema di decreto del Presidente del Consiglio dei ministri recante regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza (Atto n. 240).

Ricorda quindi che il termine per l'espressione del parere è fissato al 13 febbraio prossimo.

Francesco BERTI (M5S), *relatore per la I Commissione,* intervenendo da remoto, osserva preliminarmente come lo schema di decreto in esame sia stato predisposto in attuazione delle previsioni del comma 3 dell'articolo 1 del decreto-legge n. 105 del 2019, che demanda a un apposito decreto del Presidente del Consiglio dei ministri, da adottarsi su proposta del Comitato interministeriale per la sicurezza della Repub-

blica (CISR) entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto-legge, la definizione – con annessa disciplina dei termini e delle modalità attuative – delle procedure in base alle quali i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica notificano al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici inclusi nel perimetro e le misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici suddetti, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

A sua volta, il comma 4-*bis* del medesimo articolo 1 prevede che lo schema di decreto sia trasmesso alla Camera dei deputati e al Senato della Repubblica per l'espressione del parere delle Commissioni parlamentari competenti per materia, che si pronunciano nel termine di trenta giorni, decorso il quale il decreto può essere comunque adottato. I medesimi schemi sono altresì trasmessi al Comitato parlamentare per la sicurezza della Repubblica.

Relativamente al termine di adozione dello schema in esame, come ricordato anche dal Consiglio di Stato nel parere espresso sul provvedimento, l'articolo 1, comma 3, del decreto-legge n. 105 del 2019 prevede che il decreto attuativo ivi previsto debba essere adottato « entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto » (ossia entro dieci mesi dal 21 novembre 2019, data di entrata in vigore della legge di conversione 18 novembre 2019, n. 133). Il termine sarebbe dunque venuto a scadenza il 21 ottobre 2020. Tuttavia l'articolo 103, comma 1, del decreto-legge n. 18 del 2020, in considerazione dell'emergenza Covid-19, ha stabilito che « ai fini del computo dei termini ordinatori o perentori, propedeutici, endoprocedimentali, finali ed esecutivi, relativi allo svolgimento di procedimenti amministrativi su istanza di parte o d'ufficio, pendenti alla data del 23 febbraio 2020 o iniziati successivamente a tale data, non si tiene conto del periodo compreso tra la medesima data e quella del 15 aprile 2020 ». Successivamente, l'articolo 37 del decreto-legge n. 23 del 2020 ha prorogato il suddetto termine al 15 maggio 2020.

Il Consiglio di Stato ha rilevato come ritenga che tale periodo di sospensione sia applicabile anche al termine per l'adozione dei regolamenti. Ne consegue – osserva il Consiglio di Stato – che il termine ultimo utile per l'adozione del decreto in esame deve ritenersi prorogato *ex lege* di 81 giorni (pari al periodo di sospensione, dal 23 febbraio al 15 maggio 2020).

Il termine per l'espressione del parere da parte delle competenti Commissioni parlamentari è fissato in 30 giorni, in scadenza il 13 febbraio 2021.

Per quanto riguarda il quadro normativo vigente in materia di sicurezza cibernetica, ricorda che esso è stato definito, da ultimo, dal decreto-legge n. 105 del 2019 e, in attuazione di questo, dal decreto del Presidente del Consiglio dei ministri n. 131 del 2020 in materia di perimetro di sicurezza cibernetica e dal decreto del Presidente del Consiglio dei ministri 8 agosto 2019 che ha dettato disposizioni sul CSIRT italiano (*Computer security incident response team*).

Tale decreto, come quello in esame, è aggiornato – con cadenza almeno biennale – con la medesima proceduta prevista per la relativa adozione, in base alle previsioni del decreto-legge n. 105 del 2019.

Ricorda, inoltre, che gli interventi per il rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese previste dal perimetro di sicurezza nazionale cibernetica (di cui al decreto-legge n. 105 del 2019), dalla direttiva NIS (attuata con il decreto legislativo n. 65 del 2018) e dalle iniziative previste dalla strategia Europea di *Cybersecurity* del 16 dicembre 2020, inclusa l'applicazione del *Cybersecurity Act* (*Regulation* EU 2019/881) sono richiamati espressamente nello schema di Piano nazionale di ripresa e resilienza trasmesso al Parlamento nel gennaio 2021. In tale ambito si richiama l'obiettivo di « migliorare la resilienza dell'infrastruttura IT del nostro Paese, irrobustendo gli strumenti digitali e le competenze specialistiche necessari a

garantire la continuità operativa partendo dalle funzioni e servizi essenziali dello Stato il cui malfunzionamento potrebbe creare un pregiudizio alla sicurezza nazionale ed europea ». Lo stanziamento totale per questo progetto è di circa 1.250 milioni si euro, di cui circa 50 milioni già stanziati per la realizzazione di un *data center* del Ministero dell'Interno e per il potenziamento delle reti di connettività delle strutture operatrici del CNVVF.

Per quanto attiene al contenuto dello schema di regolamento in esame, il quale è composto da 11 articoli, suddivisi in quattro Capi e due Allegati, il Capo I, recante le Disposizioni generali, è composto dall'articolo 1, che contiene le definizioni utilizzate nell'articolato, ritenute necessarie a chiarire la portata delle disposizioni contenute nello schema decreto, soffermandosi, in particolare, su quei termini, o locuzioni, ai quali sono stati attribuiti, ai fini del decreto in esame, significati tecnici specifici, nell'ottica di garantire la coerenza con l'assetto definitorio delineato dagli altri provvedimenti di attuazione del decreto-legge.

Richiama, in particolare le seguenti definizioni:

soggetti inclusi nel perimetro (di cui alla lettera *c)*): soggetti che siano stati individuati secondo le procedure di cui all'articolo 1, comma 2, lettera *a)*, del decreto-legge n. 105 del 2019, e inclusi nell'elencazione contenuta nell'atto amministrativo adottato ai sensi dell'articolo 1, comma 2-*bis*, del medesimo decreto-legge;

rete, sistema informativo (di cui alla lettera *e)*):

1) una rete di comunicazione elettronica ai sensi dell'articolo 1, comma 1, lettera *dd)*, del decreto legislativo n. 259 del 2003 (ossia sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportata);

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali, ivi inclusi i sistemi di controllo industriale;

3) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1 e 2), per il loro funzionamento, uso, protezione e manutenzione, compresi i programmi di cui al punto 2);

servizio informatico (di cui alla lettera *f)*): il servizio consistente interamente o prevalentemente nel trattamento di informazioni, per mezzo della rete e dei sistemi Informativi, ivi incluso quello di *cloud computing*;

bene ICT (di cui alla lettera *g)*): (*information and communication technology*): insieme di reti, sistemi informativi e servizi informatici, o parti di essi, incluso nell'elenco di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge n. 105 del 2019. Si tratta dell'elenco che i soggetti inclusi nel perimetro predispongono e aggiornano, con cadenza almeno annuale, recante i beni ICT di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono (articolo 7 del decreto del Presidente del Consiglio dei ministri n. 131 del 2020);

impatto sul bene ICT (di cui alla lettera *i)*): limitazione della operatività del bene ICT, ovvero compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali; la definizione rileva ai fini dell'operatività della disposizione di cui all'articolo 11, comma 3, lettera *a)*, del decreto-

legge n. 105 del 2019, che impone l'obbligo di notifica al CSIRT italiano per gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui al comma 2, lettera *b)* del medesimo decreto-legge n. 105.

Il Capo II, composto dagli articoli da 2 a 6, disciplina le notifiche da incidente, con particolare riguardo agli incidenti aventi impatto su beni ICT, alla notifica volontaria degli incidenti, alla trasmissione delle notifiche e ad incidenti attinenti alla gestione delle informazioni classificate.

In tale ambito si prevede, in sintesi, che – al verificarsi di uno degli incidenti elencati, aventi impatto in particolare su beni ITC – i soggetti inclusi nel perimetro sono tenuti a procedere alla notifica al CSIRT italiano (*Computer security incident response team*) tramite appositi canali di comunicazione entro 6 ore o entro 1 ora in base alla tipologia di incidente.

Una volta definiti e avviati i piani di attuazione delle attività per il ripristino è data comunicazione al medesimo CSIRT italiano ed è trasmessa, se richiesta, una relazione tecnica sugli elementi significativi dell'incidente e sulle azioni adottate per porvi rimedio. Il DIS inoltra successivamente le notifiche ai competenti soggetti della struttura di governo. È altresì consentito, ai medesimi soggetti, di procedere ad una notifica su base volontaria di incidenti non ricompresi nell'elenco dello schema di decreto.

Più nel dettaglio, l'articolo 2, recante la tassonomia degli incidenti, rinvia alle tabelle n. 1 e n. 2 dell'allegato A del provvedimento, che recano la classificazione degli incidenti aventi impatto sui beni ICT. Le due tabelle sono distinte a seconda della gravità degli incidenti, essendo elencati i meno gravi nella prima e i più gravi nella seconda, anche tenuto conto della tempistica necessaria per una risposta efficace.

L'articolo 3, che disciplina l'obbligo e le modalità di notifica a seguito di incidenti, stabilisce, al comma 1, che i soggetti inclusi nel perimetro, al verificarsi di uno degli incidenti avente impatto su un bene ICT di rispettiva pertinenza individuati nelle tabelle di cui all'allegato A dello schema di decreto procedono alla notifica al CSIRT italiano.

Inoltre, in base al comma 2, i soggetti inclusi nel perimetro procedono a tale notifica anche nei casi in cui uno degli incidenti individuati nelle tabelle di cui all'allegato A abbia comunque impatto su un bene ICT di rispettiva pertinenza, ancorché si verifichi a carico di un sistema informativo, ovvero (di) un servizio informatico, o parti di essi, che, anche in esito all'analisi del rischio condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero *software* di base quali sistemi operativi e di virtualizzazione.

L'analisi di rischio è effettuata ai sensi dell'articolo 7, comma 2, del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, recante il Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge n. 105 del 2019, il quale dispone che, una volta ricevuta la relativa comunicazione, i soggetti inclusi nel perimetro, in esito all'analisi del rischio, per ogni funzione essenziale o servizio essenziale provvedono ad individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale.

A tale fine sono valutati:

1) l'impatto di un incidente sul bene ICT, in termini sia di limitazione della operatività del bene stesso, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali;

2) le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione.

Riguardo alla formulazione del comma 2, per declinare con maggiore chiarezza l'obbligo ivi previsto, nel parere del Consiglio di Stato reso sullo schema in esame, si rappresenta l'opportunità di riformulare la disposizione nei seguenti termini: « I soggetti inclusi nel perimetro procedono alla

notifica di cui al comma 1 anche nei casi in cui uno degli incidenti individuati nelle tabelle di cui all'allegato A si verifichi a carico di un sistema informativo o un servizio informatico, o parti di essi, che condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero software di base, quali sistemi operativi e di virtualizzazione ».

Le modalità della notifica sono previste dal comma 3, il quale dispone che si proceda tramite appositi « canali di comunicazione » del CSIRT italiano aventi i requisiti previsti dal decreto legislativo n. 65 del 2018 e secondo le modalità definite dal CSIRT italiano e rese disponibili sul sito Internet del CSIRT italiano secondo i termini ivi previsti.

In base all'allegato I, punto 1, lettera *a)*, del decreto legislativo n. 65 del 2018, tra i requisiti del CSIRT è previsto che sia tenuto a garantire un alto livello di disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e disponga di vari mezzi che permettono allo stesso di essere contattato e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano.

I termini per la notifica sono così individuati:

a) entro il termine di sei ore dal momento in cui il soggetto incluso nel perimetro è venuto a conoscenza di uno degli incidenti individuati nella tabella 1 di cui all'allegato A;

b) entro il termine di un'ora dal momento in cui il soggetto incluso nel perimetro è venuto a conoscenza di uno degli incidenti individuati nella tabella 2 di cui all'allegato A.

Per esigenze di qualità del testo normativo, nel parere del Consiglio di Stato si rappresenta l'opportunità di riformulare il comma 3 nei seguenti termini: « La notifica deve essere effettuata entro sei ore dal momento in cui il soggetto incluso nel perimetro è venuto a conoscenza di uno degli incidenti individuati nella tabella 1 di cui all'allegato A ed entro un'ora nel caso di incidenti individuati nella tabella 2 di cui all'allegato medesimo. La notifica è effettuata tramite appositi canali di comunicazione del CSIRT italiano aventi i requisiti di cui al punto 1, lettera *a)*, dell'allegato I, del decreto legislativo n. 65 del 2018, e secondo le modalità definite dal CSIRT italiano e rese disponibili sul sito Internet del CSIRT italiano ».

Il comma 4 dispone inoltre che, qualora il soggetto incluso nel perimetro venga a conoscenza di nuovi elementi significativi la notifica di è integrata tempestivamente (nel parere del Consiglio di Stato si rileva l'opportunità di sostituire tale avverbio con « immediatamente ») dal momento in cui il soggetto incluso nel perimetro ne è venuto a conoscenza, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

Tra i nuovi elementi significativi si richiamano nel testo le specifiche vulnerabilità sfruttate, la rilevazione di eventi comunque correlati all'incidente oggetto di notifica, ovvero gli indicatori di compromissione (IOC). Al riguardo, rileva l'opportunità di introdurre una definizione di tali indicatori di compromissione, come evidenziato anche nel parere reso dal Consiglio di Stato.

Il comma 5 prevede altresì che gli operatori di servizi essenziali e i fornitori di servizi digitali (di cui agli articoli 12 e 14 del decreto legislativo n. 65 del 2018) con la notifica ai sensi dell'articolo 3 in esame sono tenuti a comunicare che la stessa costituisce anche adempimento dell'obbligo di notifica di cui, rispettivamente, agli articoli 12, comma 5, indicando a tal fine l'autorità competente NIS alla quale la notifica deve essere inoltrata, e 14, comma 4, del decreto legislativo n. 65 del 2018.

Ricorda che in base all'articolo 12, comma 5, gli operatori di servizi essenziali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.

Ai sensi dell'articolo 14, comma 4, i fornitori di servizi digitali notificano al CSIRT italiano e, per conoscenza, all'autorità competente NIS, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla fornitura di un servizio di cui all'allegato III che essi offrono all'interno dell'Unione europea.

Nel parere del Consiglio di Stato si ricorda che l'autorità competente NIS è definita dall'articolo 3 del decreto legislativo n. 65 del 2018 che dispone: « Ai fini del presente decreto si intende per: *a)* autorità competente NIS, l'autorità competente per settore, in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1 », mentre non risulta invece definita nell'articolo 1 dello schema di decreto. Si rileva pertanto l'opportunità di integrare l'elenco delle definizioni dell'articolo 1 (con un rinvio alla norma primaria ora citata) oppure di inserire tale rinvio nel testo del comma 5.

Si prevede inoltre che le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico (di cui all'articolo 16-*ter*, comma 2, del codice delle comunicazioni elettroniche di cui al decreto legislativo n. 259 del 2003), con la notifica in questione, comunicano che la stessa costituisce anche adempimento dell'obbligo previsto ai sensi dell'articolo 16-*ter* del codice delle comunicazioni elettroniche e delle correlate disposizioni attuative.

Si stabilisce infine che restano fermi, per le notifiche degli incidenti non rientranti nell'ambito di applicazione del decreto-legge, gli obblighi e le procedure di notifica previsti dal decreto legislativo n. 65 del 2018 (di attuazione della direttiva NIS) e dal Codice delle comunicazioni elettroniche (di cui al decreto legislativo n. 259 del 2003).

È previsto altresì, al comma 6, che, su richiesta del CSIRT italiano, il soggetto incluso nel perimetro che ha proceduto a effettuare una notifica provvede, tramite i canali di comunicazione (di cui al comma 3) ed entro sei ore dalla richiesta, a effettuare un aggiornamento della notifica, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

In base al comma 7, una volta « definiti e avviati » i piani di attuazione delle attività per il ripristino dei beni ICT impattati dall'incidente oggetto di notifica, il soggetto incluso nel perimetro che ha proceduto a effettuare una notifica ai sensi delle suddette disposizioni, tramite i canali di comunicazione di cui al comma 3, ne da tempestiva comunicazione al CSIRT italiano, trasmettendo, altresì, su richiesta del CSIRT italiano ed entro 30 giorni dalla stessa richiesta, una relazione tecnica che illustra gli elementi significativi dell'incidente, tra cui le conseguenze dell'impatto sui beni ICT derivanti dall'incidente e le azioni intraprese per porvi rimedio, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa. Al riguardo segnala l'opportunità di specificare il soggetto competente alla definizione dei piani.

I soggetti inclusi nel perimetro, ai sensi del comma 8, sono tenuti inoltre « ad assicurare che dell'avvenuta notifica sia fornita notizia all'articolazione per l'implementazione del perimetro prevista nell'allegato B (sottocategoria 2.1.4 (ID.AM-6)) ».

Nel parere del Consiglio di Stato si ricorda che la disposizione di cui al comma 8 dell'articolo 3 intende evidentemente stabilire che della notifica dell'incidente sia informata la struttura di *cybersecurity* interna al soggetto (incluso nel perimetro) che ha subito l'incidente (e che ha quindi effettuato la notifica). Si evidenzia come la formulazione del comma 8 appaia tuttavia poco chiara, considerato che la voce (categoria) 2.1 dell'allegato B riguarda, nell'ambito delle misure di sicurezza, le modalità di organizzazione e gestione delle apposite strutture (dei soggetti ricompresi nel perimetro) di « Gestione degli asset (*Asset Management*) (ID.AM) », finalizzate ad assicurare – come precisato nell'allegato citato – che « i dati, il personale, i dispositivi, i sistemi e le *facility* necessari all'organizzazione siano identificati e gestiti in coerenza

con gli obiettivi e con la strategia di rischio dell'organizzazione ».

Più in particolare, la voce (sottocategoria) 2.1.4 (ID.AM-6) riguarda la definizione dei ruoli e delle responsabilità inerenti la *cybersecurity* per tutto il personale e per eventuali terze parti rilevanti (fornitori, clienti, partner). Nel parere si chiede dunque che la disposizione – di cui all'articolo 3, comma 8, così come di cui all'articolo, 4 comma 4 – sia riformulata con una più esplicita e diretta indicazione dell'oggetto cui essa riferisce, alla quale potrà aggiungersi anche il rinvio alla corrispondente voce dell'allegato 2, non essendo sufficiente la mera indicazione del codice identificativo di tale voce (categoria e sottocategoria identificative della misura di sicurezza).

L'articolo 4 disciplina la notifica volontaria degli incidenti, stabilendo che, al di fuori dei casi di cui all'articolo 3, i soggetti inclusi nel perimetro hanno facoltà di notificare, su base volontaria, gli incidenti relativi ai beni ICT, non indicati nelle tabelle di cui all'allegato A, ovvero gli incidenti, indicati nelle tabelle di cui all'allegato A, relativi a reti, sistemi informativi e servizi informatici di propria pertinenza diversi dai beni ICT.

Si precisa, al comma 2, che le notifiche volontarie sono trattate dal CSIRT in subordine a quelle obbligatorie e qualora ciò non costituisca un « onere sproporzionato o eccessivo ».

In ogni caso, ai sensi del comma 3 la notifica volontaria « non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica ».

Il comma 4 prevede, anche per le notifiche volontarie che i soggetti inclusi nel perimetro assicurano che dell'avvenuta notifica sia fornita notizia all'articolazione per l'implementazione del perimetro prevista nell'ambito delle misure di sicurezza di cui all'allegato B (sottocategoria 2.1.4 (ID.AM-6). Nel parere del Consiglio di Stato si evidenzia che occorre chiarire se la « notifica volontaria » debba essere effettuata attraverso gli stessi canali dedicati previsti per la notifica obbligatoria dall'articolo 3 e si invita a valutare « se non sia preferibile e opportuno qualificare tale "notifica volontaria" con il diverso termine "informativa volontaria" o "comunicazione volontaria", eventualmente specificando modalità alternative e semplificate di comunicazione, posto che, come esplicitato nel comma 2, nessun obbligo ulteriore può derivare da tale iniziativa in capo al soggetto che effettua la comunicazione » Inoltre, nel medesimo parere si sottolinea la necessità di riformulare il comma 3 nei seguenti, più semplici termini: « Dalla notifica volontaria non deriva alcun obbligo di ulteriori adempimenti a carico del soggetto notificante » e si richiama, in ordine al comma 4, quanto evidenziato con riferimento all'articolo 3, comma 8.

L'articolo 5 disciplina la trasmissione delle notifiche, stabilendo in primo luogo che il DIS inoltra le notifiche ricevute ai sensi dell'articolo 3. Al riguardo segnala l'opportunità di prevedere espressamente, all'articolo 3, l'obbligo di notifica al DIS, richiamato dalla disposizione in esame.

Nel parere del Consiglio di Stato si evidenzia in proposito che manca nella sequenza logico-giuridica dell'articolato, così come costruito nello schema in esame, il passaggio precedente e pregiudiziale, previsto nell'articolo 1, comma 3, lettera *a)*, del decreto-legge n. 105 del 2019, per cui il « Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano, [che] inoltra tali notifiche, tempestivamente, al Dipartimento delle informazioni per la sicurezza anche per le attività demandate al Nucleo per la sicurezza cibernetica ». È vero – sottolinea il Consiglio di Stato – che il CSIRT italiano non è che un organismo interno al DIS (istituito ai sensi dell'articolo 8 del decreto legislativo n. 65 del 2018). Tuttavia – prosegue il Consiglio di Stato – avendo la legge previsto espressamente questo passaggio (ancorché « interno »), si reputa corretto farne menzione, per completezza, anche nel regolamento. Occorre, dunque, inserire – conclude il Consiglio di Stato – una disposizione che attui (o, quanto meno, richiami) il predetto passaggio normativo, chiarendo che il CSIRT italiano trasmette immediatamente al DIS le notifiche ricevute.

Il DIS, ai sensi del medesimo articolo 5, inoltra altresì le notifiche volontarie di cui dell'articolo 4 nel caso in cui queste vengano trattate da:

a) dall'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione (previsto dall'articolo 7-*bis* del decreto-legge n. 144 del 2005);

b) dalla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, qualora le stesse provengano da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo n. 82 del 2005, fatta eccezione per quelle concernenti i beni ICT in relazione ai quali per le attività di ispezione e verifica sono competenti le strutture specializzate di cui all'articolo 1, comma 6, lettera *c)*, terzo periodo, del decreto-legge n. 105 del 2019;

c) dal Ministero dello sviluppo economico qualora le stesse provengano da un soggetto privato.

Si prevede infine che il CSIRT italiano inoltri le notifiche ricevute dai soggetti inclusi nel perimetro, che siano identificati anche quali soggetti di cui agli articoli 12 e 14 del decreto legislativo n. 65 del 2018, all'autorità competente NIS indicata ai sensi dell'articolo 3, comma 5.

Le modalità per gli inoltri delle notifiche da parte del DIS e del CSIRT italiano previste dal medesimo articolo 5 possono essere concordate mediante apposite intese con ciascuna delle amministrazioni interessate e, tenuto anche conto di quanto previsto dall'articolo 8, comma 4, con il Ministero della difesa.

L'articolo 6 riguarda, più in particolare, gli incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate.

In questo caso, per la notifica degli incidenti relativi alle reti, ai sistemi informativi e ai servizi informati attinenti alla gestione delle informazioni classificate, non inclusi nell'elenco dei beni ICT ai sensi del decreto-legge n. 105 del 2019, resta fermo quanto previsto dal regolamento – di cui all'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007 e correlate disposizioni attuative – che prevede che il DIS assicuri l'attuazione delle disposizioni impartite dal Presidente del Consiglio dei Ministri, ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza, vigilando altresì sulla loro corretta applicazione.

Emanuele SCAGLIUSI (M5S), *relatore per la IX Commissione*, proseguendo nell'illustrazione dello schema di decreto in esame, rileva come il Capo III, composto dagli articoli da 7 a 11, disciplina le misure di sicurezza.

In particolare, l'articolo 7 è rubricato proprio « Misure di sicurezza », le quali sono articolate in: funzioni, categorie, sottocategorie, punti e lettere, individuate nell'allegato B del decreto in esame. L'insieme delle misure, di carattere tecnico e organizzativo, volte a garantire elevati livelli di sicurezza dei beni ICT, sono riportate sistematicamente nel predetto allegato e si integrano con gli ambiti già previsti dalla legislazione primaria. Tra questi, a titolo esemplificativo, vi sono quelli relativi: « alla struttura organizzativa preposta alla gestione della sicurezza », « alle politiche di sicurezza e alla gestione del rischio », alla « sicurezza fisica e logica e dei dati ».

Per la definizione delle misure, come accennato in precedenza, è stato assunto quale base di riferimento il « *Framework* nazionale per la *cybersecurity* e la *data protection* », edizione 2019.

Le misure, secondo quanto si ricava dall'allegato B, secondo quanto già accennato in precedenza, sono state organizzate in maniera sistematica in funzioni, categorie e sottocategorie ognuna delle quali è identificata anche da un codice univoco alfanumerico corrispondente alle analoghe misure del « *Framework* nazionale per la *cybersecurity* e la *data protection* », edizione 2019.

Per quanto concerne tale articolo 7 e la cosiddetta « legenda » dell'allegato 2, ricorda che il Consiglio di Stato, nel parere reso, ha evidenziato l'opportunità, per una

più agile lettura del testo, di inserire una più puntuale denominazione della rubrica dell'indice dell'allegato 2, in modo da chiarire che le funzioni sono costituite da macroaree.

L'articolo 8 disciplina le modalità e i termini di adozione delle misure di sicurezza.

Nello specifico, per i soggetti inclusi nel perimetro che debbono adottare, per ciascun bene ICT di rispettiva competenza, le misure contenute nell'allegato B sono previsti due differenti termini temporali per l'adozione delle misure stesse: 6 mesi e 24 mesi. In particolare, i termini sono distinti a seconda che si tratti di misure di più immediata attuazione o di misure per le quali l'implementazione richieda interventi maggiormente impegnativi sotto il profilo progettuale e programmatico.

Al fine di agevolare l'individuazione dei relativi termini, nello stesso allegato B è contenuta una suddivisione in due macro categorie.

La prima categoria, denominata categoria A include tutti gli interventi per i quali il termine di adozione delle misure è di 6 mesi, mentre la seconda categoria, denominata categoria B elenca gli interventi per i quali il termine è di 24 mesi.

Per quanto concerne la data di decorrenza del periodo entro il quale dovranno essere adottate le misure di sicurezza, è utile ricordare che i soggetti per i quali è previsto l'obbligo di predisporre l'elenco dei beni ICT di rispettiva pertinenza debbono trasmettere tale elenco entro il termine di 6 mesi dalla data nella quale è intervenuta la comunicazione di inclusione nel perimetro di sicurezza nazionale cibernetica.

In occasione della predisposizione dei suddetti elenchi ciascuno dei soggetti incluso nel perimetro può effettuare una analisi del rischio per ogni funzione essenziale dello Stato esercitata o servizi essenziali prestati in modo da valutare l'adozione delle misure di sicurezza per ciascuno dei beni ICT individuati in questo elenco.

Pertanto, il termine di 6 o 24 mesi per l'adozione delle misure di sicurezza contenute nelle categorie A e B decorre dalla data di trasmissione, che avverrà attraverso la piattaforma digitale costituita presso il DIS, dei richiamati elenchi dei beni ICT.

Per quanto riguarda le comunicazioni che i soggetti obbligati dovranno trasmettere mediante la predetta piattaforma digitale, nell'articolo sono disciplinate le relative modalità.

In particolare, si dispone che il DIS dovrà rendere tempestivamente disponibili le comunicazioni ricevute alla struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione e al Ministero dello Sviluppo economico affinché possano essere svolte le rispettive attività di verifica e ispezione.

Per quanto concerne, invece, le attività di ispezione e verifica per i beni ICT legati alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine della sicurezza pubblica, alla difesa civile, alla difesa nazionale e alla sicurezza militare dello Stato, poiché le verifiche e le ispezioni dovranno essere svolte dalle competenti strutture dell'amministrazione da cui dipendono le forze di polizia e le forze armate, viene escluso che le comunicazioni sulle misure di sicurezza relative ai beni ICT vengano – successivamente alla trasmissione e conservazione sulla piattaforma digitale del DIS – rese disponibili alle citate strutture della Presidenza del Consiglio dei ministri e del Ministro dello sviluppo economico.

L'articolo 9 è dedicato alla tutela delle informazioni, individuando nell'allegato C dello schema di decreto le misure minime di sicurezza di natura tecnica e organizzativa che sono volte a tutelare le informazioni relative all'elenco dei soggetti inclusi nel perimetro, all'elenco dei beni ICT e agli elementi delle notifiche di incidente.

Le misure in questione sono state suddivise in due macro categorie: la prima relativa ai trattamenti svolti con l'ausilio di strumenti elettronici; la seconda concernente le misure di sicurezza fisica e documentale.

Al fine di garantire in tempi celeri la tutela delle informazioni in questione, qualora queste ultime non richiedano partico-

lari interventi da parte dei soggetti tenuti al loro rispetto, è previsto che le disposizioni volte a tutelare la sicurezza delle informazioni stesse debbano essere applicate entro 60 giorni dall'entrata in vigore del decreto in esame.

Viene inoltre prevista una clausola di salvaguardia per l'adozione da parte dei soggetti inclusi nel perimetro di ulteriori e più elevati livelli di sicurezza delle misure contenute nell'allegato B.

Segnala, inoltre, che qualora delle informazioni riguardanti uno degli ambiti oggetto dell'applicazione di misure minime di cui all'allegato C relative alla tutela dell'informazione venga attribuita una classificazione di segretezza in base alla normativa vigente (articolo 42 della legge n. 124 del 2007), troverà applicazione la disciplina regolamentare attuativa della suddetta legge.

L'articolo 10, al fine di assicurare una maggiore chiarezza tra le diverse norme ordinamentali di settore, precisa che le misure di sicurezza previste dal decreto in questione non si applicano alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate, in ragione della loro esclusione dall'elenco dei beni ICT.

L'articolo 11 reca la clausola di invarianza finanziaria, precisando che dal decreto in esame non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.

Giuseppe BRESCIA, *presidente*, nessun altro chiedendo di intervenire, rinvia il seguito dell'esame da altra seduta.

La seduta termina alle 13.45.