N. 01357/2020 AFFARE

Numero 00028/2021 e data 11/01/2021 Spedizione

Firmato digitalmente

REPUBBLICA ITALIANA

Consiglio di Stato

Sezione Consultiva per gli Atti Normativi

Adunanza di Sezione del 1 dicembre 2020

NUMERO AFFARE 01357/2020

OGGETTO:

Presidenza del consiglio dei ministri - Dipartimento per gli affari giuridici e legislativi.

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*", in attuazione dell'articolo 1, comma 3, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

LA SEZIONE

Vista la nota di trasmissione n. prot. 11356 del 18 settembre 2020 con la quale la Presidenza del Consiglio dei ministri - Dipartimento per gli affari giuridici e

legislativi ha trasmesso lo 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*", in attuazione dell'articolo 1, comma 3, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;

Esaminati gli atti e udito il relatore, consigliere Paolo Carpentieri;

Premesso:

1. Il decreto-legge 21 settembre 2019, n. 105, recante *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, ha istituito, nell'art. 1, il *perimetro di sicurezza nazionale cibernetica*, al fine di *assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati 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, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.*

2. Lo schema di decreto in esame attua in particolare le previsioni del comma 3 dell'articolo 1 citato, che demanda a un apposito decreto del Presidente del consiglio dei ministri, da adottarsi su proposta del Comitato interministeriale per la sicurezza della Repubblica (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): a) 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; b) delle 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 riguardo ai seguenti settori di attività e profili (definiti anche "*ambiti*" nell'ultimo *Considerato* del preambolo dello schema di decreto, nella relazione illustrativa e nell'articolo 7, comma 1): struttura organizzativa preposta alla gestione della sicurezza, politiche di sicurezza, gestione del rischio, mitigazione e gestione degli incidenti e loro prevenzione, protezione fisica e logica e dei dati, integrità delle reti e dei sistemi informativi, gestione operativa, monitoraggio, test e controllo, formazione e consapevolezza, affidamento di forniture di beni, sistemi e servizi ICT.

3. Lo schema di decreto si compone complessivamente di 11 articoli ed è suddiviso in quattro Capi. Il Capo I è dedicato alle "*Disposizioni generali*", il Capo II alle "*Notifiche di incidente*", il Capo III alle "*Misure di sicurezza*" e il Capo IV alle "*Disposizioni finali*". Le "*Disposizioni generali*" si risolvono nel solo articolo 1, recante le definizioni (correttamente concordanti con quelle della legge e con quelle già previste nei precedenti, citati, decreti attuativi). Il Capo II, sulle *Notifiche di incidente*, comprende gli articoli 2 (*Tassonomia degli incidenti*), 3 (*Notifica degli incidenti aventi impatto su beni ICT*), 4 (*Notifica volontaria degli incidenti*), 5 (*Trasmissione delle notifiche*) e 6 (*Incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate*). Il Capo III riguarda le "*Misure di sicurezza*" e comprende gli articoli 7 (*Misure di sicurezza*), 8 (*Modalità e termini di adozione delle misure di sicurezza*), 9 (*Tutela delle informazioni*) e 10 (*Misure di sicurezza relative alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate*). Il Capo IV ("*Disposizioni finali*") è costituito dal solo articolo 11 (*Disposizioni finali*) che si risolve nella clausola di invarianza della spesa.

4. L'articolato è completato da tre allegati: l'allegato A, previsto dall'articolo 2, che reca la tassonomia degli incidenti; l'allegato B, previsto dall'articolo 7, che reca le misure di sicurezza (con due appendici: l'appendice n. 1, costituita da una tabella di corrispondenza tra gli ambiti di cui all'articolo 1, comma 3, lettera *b*), del decreto-legge e le misure di sicurezza dell'allegato B, nonché l'appendice n. 2, costituita da una tabella di corrispondenza tra le misure di sicurezza e le categorie A - B); l'allegato C, previsto dall'articolo 9, che reca le misure minime di sicurezza per la tutela delle informazioni.

5. Il testo è corredato di relazione tecnica, di analisi tecnico-normativa (ATN), di stralcio del verbale del Comitato interministeriale per la sicurezza della Repubblica - CISR del 27 ottobre 2020. Il testo non è invece corredato di analisi di impatto della regolazione (AIR) poiché ne è richiesta l'esclusione, ai sensi dell'articolo 6, comma 1, del d.P.C.M. n. 169 del 2017 (con nota del Capo del Dipartimento per gli affari giuridici e legislativi), con la motivazione che "*il provvedimento in esame concerne misure necessarie per la sicurezza interna dello Stato*".

6. La relazione illustrativa informa, circa l'*iter* elaborativo del testo, che sono stati costituiti appositi gruppi di lavoro, che hanno visto la partecipazione dei rappresentanti delle diverse amministrazioni interessate, e che la condivisione tra le amministrazioni sulle diverse soluzioni tecnico-giuridiche elaborate e, quindi, sullo schema di decreto è stata, poi, assicurata nell'ambito dell'organismo tecnico di supporto al CISR di cui all'articolo 4, comma 5, del regolamento adottato con d.P.C.M. 3 aprile 2020, n. 2 (il c.d. "CISR tecnico"), integrato da un rappresentante della struttura della Presidenza del Consiglio competente per la innovazione tecnologica e la digitalizzazione, designato in ragione degli specifici compiti attribuiti alla Presidenza del consiglio dal decreto-legge, nonché da rappresentanti del Ministero delle infrastrutture e dei trasporti, del Ministero del lavoro e delle politiche sociali, del Ministero dell'università e ricerca, nonché dell'Ufficio del Consigliere militare del Presidente del Consiglio dei ministri. Sullo schema di

decreto è infine intervenuto il CISR - organo al quale compete la proposta di adozione - che ha favorevolmente deliberato sul testo, in via preliminare, nella seduta del 27 ottobre 2020.

Considerato:

I. Considerazioni generali

1. La norma primaria (art. 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 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, 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 legge 8 aprile 2020, n. 23, convertito, con modificazioni, dalla legge 5 giugno 2020, n. 40, ha prorogato il suddetto termine al 15 maggio 2020. Il Collegio ritiene che tale periodo di sospensione sia applicabile anche al termine per l'adozione dei regolamenti. Ne consegue 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).

2. Il Collegio rileva che molti degli "incidenti" rilevanti contemplati dal presente schema di decreto rientrerebbero nell'ambito della casistica di violazione dei dati personali ("*Data Breach*") soggetta a notifica all'autorità di controllo ai sensi dell'articolo 33 del "Gdpr" [*Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con*

riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)]. Sarebbe stato dunque necessario acquisire il parere del Garante per la protezione dei dati personali. Rileva tuttavia il Collegio che il Gdpr esclude dal suo ambito di applicazione, nell'articolo 2, paragrafo 2, i trattamenti di dati personali effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quelli effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE (*Disposizioni specifiche sulla politica estera e di sicurezza comune*), nonché quelli effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse. Sarebbe necessario che l'Amministrazione chiarisse, almeno nella relazione illustrativa, se e quali di tali ragioni rilevino nel caso in esame al fine di giustificare la mancata acquisizione del suddetto parere.

3. La Sezione ha già avuto occasione di recente di occuparsi della tematica degli strumenti attuativi dell'articolo 1 del decreto-legge n. 105 del 2019 in materia di perimetro di sicurezza nazionale cibernetica, pronunciandosi dapprima (con il parere n. 983 del 26 maggio 2020) sullo schema di decreto del Presidente del Consiglio dei ministri adottato in attuazione dell'articolo 1, comma 2, del predetto decreto-legge per la definizione degli ambiti soggettivi e oggettivi inclusi nel perimetro di sicurezza nazionale cibernetica e dei criteri di predisposizione e aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici (d.P.C.M. 30 luglio 2020, n. 131); quindi (con il parere 26 ottobre 2020, n. 1664) sullo schema di decreto del Presidente della Repubblica attuativo dell'articolo 1, comma 6, del decreto-legge n. 105 del 2019, di disciplina delle procedure, delle modalità e dei termini per le verifiche e i controlli sugli acquisti di beni e servizi ICT compresi nel perimetro (regolamento, quest'ultimo, a quel che

consta, non ancora adottato).

4. Sulla notevole complessità del quadro normativo introdotto dall'articolo 1 del decreto-legge n. 105 del 2019 – e sulla conseguente necessità di ricondurre a unità, per quanto possibile, le plurime fonti normative attuative in esso previste – la Sezione si è già espressa e non può, sul punto, che rinviarsi a quanto esplicitato nei citati, precedenti pareri vertenti su questa tematica.

5. La materia trattata – in specie per quanto attiene agli allegati – presenta un alto tasso di tecnicismo, implicante il responsabile esercizio di delicate valutazioni di discrezionalità tecnica, che non possono che essere rimesse e riservate all'Amministrazione. Il presente parere si occuperà, dunque, soprattutto (se non esclusivamente) dei profili giuridico-formali di maggiore evidenza e rilievo.

II. Esame dell'articolato.

1. Articolo 1 (*Definizioni*)

1.1. Non si hanno osservazioni da formulare, salve le eventuali integrazioni indicate nei successivi paragrafi 3.3 e 3.4.

2. Articolo 2 (*Tassonomia degli incidenti*)

2.1. Il testo del comma 1 presenta una formulazione non molto lineare. Si suggerisce la seguente riformulazione: "*Nelle tabelle n. 1 e n. 2 dell'allegato A al presente regolamento sono classificati gli incidenti aventi impatto sui beni ICT. Nella tabella n. 1 sono indicati gli incidenti meno gravi e nella tabella n. 2 quelli più gravi. Tale classificazione è funzionale alla diversa tempistica necessaria per una risposta efficace*".

2.2. Le tabelle (nn. 1 e 2) contenute nell'allegato A sono costituite ciascuna da tre colonne recanti, nella prima colonna a sinistra, un codice identificativo (ICP-A-2, ICP-A-3, ICP-A-4 e così a seguire in ordine crescente nella tabella A; ICP-B-2, ICP-B-3, ICP-B-4, *etc*., nella tabella B); in quella centrale la categoria di incidente [*Infezione (Initial exploitation), Guasto (Fault), Installazione (Establish persistence), etc*.] e nella colonna di destra una descrizione della consistenza di ciascuna specie di incidente (corrispondente al codice identificativo) rientrante

nelle diverse categorie. Sarebbe molto utile, a giudizio della Sezione, che nell'articolo 2 fosse inserito un adeguato riferimento esplicativo di rinvio alla suddetta classificazione delle diverse tipologie di incidenti, idoneo a chiarificarne la struttura logica. È inoltre necessario, almeno in calce (o in testa) alle tabelle, definire l'acronimo "ICP" del codice identificativo.

3. Articolo 3 (*Notifica degli incidenti aventi impatto su beni ICT*).

3.1. Comma 2. Come risulta bene chiarito nella relazione tecnica, il decreto impone di notificare, tramite appositi canali di comunicazione del CSIRT italiano, gli incidenti che abbiano impatto su un bene ICT, e "*ciò, anche nell'ipotesi in cui gli stessi incidenti, che abbiano impatto su un bene ICT, si verifichino a carico di un bene, sistema informativo o servizio informatico non incluso nel predetto elenco, ma che condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o di memoria ovvero software di base*". Questo obbligo risulta invece declinato in modo poco chiaro nel testo del comma 2 dell'articolo 3 in esame, che deve essere riformulato come segue: "*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*".

3.2. Il comma 3, per analoghe esigenze di qualità del testo normativo, deve essere riformulato come segue: "*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".

3.3. Nel comma 4, relativo all'obbligo di comunicazione degli ulteriori elementi informativi emersi sulla natura, la dinamica, gli effetti dell'incidente, l'avverbio "*tempestivamente*" – in sé privo di un utile significato normativo – deve essere sostituito con l'avverbio "*immediatamente*". Conseguentemente la frase "*dal momento in cui il soggetto incluso nel perimetro ne è venuto a conoscenza*" (al quarto e quinto rigo del comma) può essere eliminata perché ridondante. Se si intende fare uso della sigla "*IOC*" occorre fornirne un'apposita definizione nell'articolo 1.

3.4. Nel comma 5, attuativo del comma 8 dell'articolo 1 del decreto-legge n. 105 del 2019, si prevede l'obbligo di comunicazione della notifica alla "*autorità competente NIS*" ai sensi del decreto legislativo n. 65 del 2018. La "*autorità competente NIS*" – definita dall'articolo 3 del decreto legislativo n. 65 del 2018 (1. *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*") – non risulta invece definita nell'articolo 1 del presente schema di decreto. Occorrerà, pertanto, in alternativa, o integrare l'elenco delle definizioni dell'articolo 1 (con un rinvio alla norma primaria ora citata), o inserire tale rinvio nel testo del comma 5 in esame.

3.5. Il comma 8 prevede 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 alla sottocategoria 2.1.4 (ID.AM-6) dell'allegato B*". La disposizione 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). La formulazione del comma è tuttavia poco chiara. 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*). Ciò chiarito, occorre che il testo del comma in esame sia riformulato 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).

4. Articolo 4 (*Notifica volontaria degli incidenti*).

4.1. Occorre chiarire se la "*notifica volontaria*" debba essere effettuata attraverso gli stessi canali dedicati previsti per la notifica obbligatoria dall'articolo 3. Valuti inoltre l'Amministrazione 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.

4.2. Il comma 3 deve essere riformulato nei seguenti, più semplici termini: "*Dalla notifica volontaria non deriva alcun obbligo di ulteriori adempimenti a carico del soggetto notificante*".

4.3. Vale per il comma 4 quanto considerato a proposito dell'articolo 3, comma 8. In alternativa, valuti l'Amministrazione se non riformulare il comma come segue: "*Si applica il comma 8 dell'articolo 3*".

5. Articolo 5 (*Trasmissione delle notifiche*).

5.1. L'articolo 5 attua la disposizione del secondo periodo della lettera *a*), del

comma 3 dell'articolo 1 del decreto-legge n. 105 del 2019, in base alla quale "*il Dipartimento delle informazioni per la sicurezza assicura la trasmissione delle notifiche così ricevute all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, nonché alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato*". Manca, tuttavia, nella sequenza logico-giuridica dell'articolato, così come costruito nello schema di d.P.C.M. in esame, il passaggio precedente e pregiudiziale, previsto nel periodo precedente della medesima lettera *a*) citata, in base al quale 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 che il CISIRT italiano non è che un organismo interno al DIS (istituito ai sensi dell'articolo 8 del decreto legislativo n. 65 del 2018). Tuttavia, avendo la legge previsto espressamente questo passaggio (ancorché "interno"), si reputa corretto farne menzione, per completezza, anche nel regolamento. Occorre, dunque, inserire (valuti l'Amministrazione se nell'articolo 5 o precedentemente) una disposizione che attui (o, quanto meno, richiami) il predetto passaggio normativo, chiarendo che il CSIRT italiano (*Computer security incident response team*) trasmette immediatamente al DIS le notifiche ricevute.

5.2. L'alinea del comma 1 deve essere riformulato come segue: "*Il DIS inoltra le notifiche ricevute:*". Nelle lettere *b*) e *c*) la parola "*stesse*" deve essere sostituita con la parola "*notifiche*". Prima dell'attuale comma 2 deve essere quindi aggiunto il seguente comma "2. *Le notifiche volontarie, di cui all'articolo 4, sono trasmesse solo nel caso in cui siano state trattate*". L'attuale comma 2 diviene conseguentemente comma 3.

5.3. Nell'attuale comma 3 (che diventa comma 4) le parole "*per gli inoltri*" devono

essere sostituite dalle seguenti: "*di inoltro*" e le parole "*possono essere concordate*" devono essere sostituite dalle seguenti: "*sono definite*".

6. Articolo 6 (*Incidenti relativi alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate*).

Nessuna osservazione.

7. Articolo 7 (*Misure di sicurezza*).

7.1. L'articolo 7 fornisce una sorta di "legenda" dell'allegato 2, chiarendo che "*Le misure di sicurezza, articolate in funzioni, categorie, sottocategorie, punti e lettere, sono individuate nell'allegato B al presente regolamento*". Nella *Premessa* contenuta nell'allego 2 si chiarisce ulteriormente che "*Il presente allegato definisce misure volte a garantire elevati livelli di sicurezza dei beni ICT ai sensi dell'articolo 1, comma 3, lettera b), del decreto-legge, organizzate in funzioni, categorie e sottocategorie, ognuna identificata anche da un codice univoco alfanumerico corrispondente alle analoghe misure del Framework nazionale per la cybersecurity e la data protection", edizione 2019*". In proposito la Sezione rimette all'Amministrazione la verifica tecnica dell'adeguata corrispondenza tra le macro-aree di intervento individuate nell'allegato B e i nove "*ambiti*" – cui devono riferirsi le misure di sicurezza - previste espressamente dall'articolo 1, comma 3, lettera *b*), del decreto-legge n. 105 del 2019 (struttura organizzativa preposta alla gestione della sicurezza, alle politiche di sicurezza e gestione del rischio, mitigazione e gestione degli incidenti e loro prevenzione, protezione fisica e logica e dei dati, integrità delle reti e dei sistemi informativi, gestione operativa, ivi compresa la continuità del servizio, monitoraggio, test e controllo, formazione e consapevolezza, affidamento di forniture di beni, sistemi e servizi ICT).

7.2. Sarebbe comunque utile – per una più agevole lettura - una più puntuale denominazione delle rubriche dell'indice dell'allegato 2, in modo da chiarire che le *funzioni* sono costituite dalle "macro-aree" o fasi di rilevazione e reazione rispetto al verificarsi di incidenti definite dai numeri cardinali dei paragrafi (*Identificazione*

- paragrafo 2, *Protezione* – paragrafo 3, *Rilevamento* – paragrafo 4, *Risposta* – paragrafo 5, *Recupero* – paragrafo 6); che all'interno di queste "macro-aree" (*funzioni* o fasi di rilevazione) sono poi definite le *categorie* di misure di sicurezza [identificate con una sotto-numerazione (2.1, 2.2, 2.3, *etc.*), quali, ad esempio, *Gestione degli asset* (*Asset Management*) (*ID.AM*), *Governance* (*ID.GV*), *Valutazione del rischio* (*Risk Assessment*) (*ID.RA*), *Strategia della gestione del rischio* (*ID.RM*), *etc.*; che, infine, ciascuna categoria si articola al suo interno in sottocategorie (ad esempio, 2.1.1 ID.AM-1, 2.1.2 ID.AM-2, 2.1.3 ID.AM-3, *etc.*), ulteriormente suddivise in specifiche azioni.

7.3. Nel secondo periodo del comma 1 l'articolo 7 informa inoltre che *'La corrispondenza tra le misure di sicurezza e gli ambiti elencati all'articolo 1, comma 3, lettera b), del decreto-legge è indicata nella tabella in appendice n. 1 dell'allegato B*". Non è questa la sede per entrare nel merito delle scelte redazionali e di strutturazione logica dell'allegato compiute dall'Amministrazione (evidentemente dettate dall'esigenza di riprendere le classificazioni usate nel *Framework* nazionale per la *cybersecurity* e la *data protection*", edizione 2019, o altro riferimento tecnico), ma è doveroso rilevare come la costruzione prescelta appaia inutilmente complicata, lì dove sarebbe stato più semplice e chiaro usare la tabella di corrispondenza come indice e radice logica all'interno della quale organizzare l'elencazione, la classificazione e la descrizione delle diverse misure di sicurezza per "*ambiti*" (come definiti dalla legge) e categorie e sottocategorie riferite a ciascuna funzione. Nella relazione illustrativa si chiarisce, circa il rapporto di corrispondenza tra le misure di sicurezza individuate dal presente decreto e i nove ambiti delineati dall'articolo 1, comma 3, lettera *b*), del decreto-legge, che "*In ragione della richiamata scelta operata nei sensi di assumere, quale base di riferimento, il Framework nazionale, e delle conseguenti ricadute redazionali e sistematiche sull'elaborazione del testo regolamentare comprensivo degli allegati, l'allegato B è corredato (in appendice n. 1) di una tabella di corrispondenza tra gli ambiti del decreto-legge e le misure individuate per ciascuno di tali ambiti. Nel*

caso in cui una misura attenga a più ambiti, la stessa è stata riportata in corrispondenza di ciascuno di essi. Nel caso in cui, infine, in relazione ad uno specifico ambito trovi applicazione soltanto una parte specifica di una determinata misura, anche tale limitazione è stata opportunamente evidenziata". È dunque evidente alla stessa Amministrazione proponente la macchinosità del sistema prescelto, evidentemente imposto dalla maggiore interoperabilità e utilità pratica del modello costituito dal "*Framework nazionale per la cybersecurity e la data protection", edizione 2019 (Framework nazionale)*", realizzato dal Centro di ricerca di *cyber intelligence and information security* (CIS) dell'Università Sapienza di Roma e dal Laboratorio nazionale di *Cybersecurity* del Consorzio interuniversitario nazionale per l'informatica (CINI), con il supporto dell'Autorità garante per la protezione dei dati personali e del Dipartimento delle informazioni per la sicurezza (DIS). Deve tuttavia evidenziarsi – lasciando ogni valutazione in merito all'Amministrazione - come la "combinazione" tra gli "*ambiti*" definiti dal legislatore e la ripartizione articolata in "*funzioni*" nell'allegato B lasci spazio a dubbi sulla reale corrispondenza tra queste due classificazioni e ponga obiettive difficoltà di lettura.

7.4. Sempre ai fini di una più agevole leggibilità del testo, sarebbe utile aggiungere nell'articolo 7, stante questa sua funzione esplicativa di descrizione dei contenuti dell'allegato B, una specificazione relativa all'appendice 2 contenuta nell'allegato B ora detto, appendice la cui funzione e il cui significato si ricavano solo indirettamente dal testo del successivo articolo 8. L'appendice n. 2 dell'allegato B reca, peraltro, la sintetica e poco significativa rubrica "*Categorie*", che non ne consente un'immediata comprensione (denominazione che, peraltro, rischia di ingenerare anche equivoci, rispetto alle "*categorie*" di incidenti definite nell'allegato A e rispetto alle "*categorie*" tipologiche di classificazione delle misure di sicurezza previste nell'allegato B). Sarebbe utile integrare tale rubrica con la specificazione, ricavabile dall'articolo 8, che le "*categorie*" "A" e "B" di cui

all'appendice 2 servono alla ripartizione delle misure di sicurezza agli effetti dei termini di adozione e di comunicazione dell'avvenuta adozione da parte dei soggetti inclusi nel perimetro. Potrebbe a tali fini riprendersi l'indicazione contenuta nella relazione illustrativa, nella quale le due macro-categorie in cui sono state suddivise le misure individuate nell'allegato B includono – nella "categoria" A – quelle da adottare entro 6 mesi e – nella "categoria" B – quelle da adottare entro 24 mesi.

8. Articolo 8 (*Modalità e termini di adozione delle misure di sicurezza*).

8.1. Il comma 1 prevede un unico termine per l'adozione e per la comunicazione dell'avvenuta adozione delle misure di sicurezza; sarebbe più logico prevedere o due termini diversi, o il solo termine di comunicazione dell'avvenuta adozione. Non risulta inoltre indicata l'Autorità alla quale la comunicazione deve essere destinata (il CSIRT italiano o il DIS; sembra il DIS, da quanto si può evincere dal comma 4). Sotto il profilo della tecnica redazionale del testo, conviene distinguere – come indicato anche per l'analoga previsione dell'articolo 3, comma 3 (cfr. sopra, paragrafo 3.2) - in due distinte statuizioni i due comandi giuridici contenuti nella disposizione (l'adozione e comunicazione dell'adozione delle misure di sicurezza e le modalità di comunicazione). Sarebbe dunque preferibile scindere in due commi (o in due diversi periodi) la disposizione in esame, nei seguenti termini: "1. *I soggetti inclusi nel perimetro adottano per ciascun bene ICT di rispettiva pertinenza le misure di sicurezza di cui all'allegato B nei seguenti termini: a) . . . b) . . ., etc.* 2. *I soggetti di cui al comma 1, immediatamente dopo l'avvenuta adozione delle misure di sicurezza di cui all'allegato B, ne danno comunicazione [al CSIRT italiano o al DIS], descrivendo le relative modalità, mediante la piattaforma digitale costituita presso il DIS ai sensi dell'articolo 9, comma 1, del regolamento adottato con DPCM n. 131 del 2020, con il modello reso disponibile dal DIS 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*".

8.2. Nella lettera *a*) del comma 1 è previsto che "*qualora la trasmissione avvenga*

in una data antecedente a quella di entrata in vigore del presente regolamento, [la comunicazione deve essere effettuata] *entro sei mesi da quest'ultima data*". Tale formulazione non è corretta, poiché qualunque data anteriore all'entrata in vigore del regolamento non può che essere, per definizione, passata e deve quindi essere indicata con il tempo passato del congiuntivo: "*sia avvenuta*" (e non "*avvenga*").

8.3. L'ultimo periodo della lettera *a*) deve essere riformulato come segue: "*I soggetti inclusi nel perimetro che abbiano già adottato le misure di sicurezza di cui alla categoria B dell'appendice n. 2 dell'allegato B, ne danno comunicazione indicando altresì le modalità di adozione*".

8.4. Per la lettera *b*) valgono le stesse considerazioni ora svolte per la lettera *a*). Inoltre, la parola "*quelle*", al primo rigo, va sostituita con le parole "*le misure di sicurezza*".

9. Articolo 9. (*Tutela delle informazioni*).

9.1. La norma riguarda le misure minime di sicurezza in tema di protezione fisica e logica dei dati e di integrità delle reti e dei sistemi informativi, ossia delle misure di sicurezza relative agli "*ambiti*" individuati dai numeri 3) e 4) della lettera *b*) del comma 3 dell'articolo 1 del decreto-legge n. 105 del 2019. Ora, mentre tali "macro-aree" di intervento delle misure di sicurezza – elencate nei nove numeri in cui si articola la citata lettera *b*) – sono definite "*ambiti*" nell'ultimo *Considerato* del preambolo del presente schema di decreto, nella relazione illustrativa e nell'articolo 7, comma 1 - nell'articolo 9 in esame, invece, si parla (ancora una volta) di "*categorie*" ("*di cui all'articolo 1, comma 3, lettera b), numeri 3 e 4, del decreto-legge*"). Come già segnalato sopra, nel paragrafo 7.4 a proposito dell'articolo 7, vi è un uso eccessivo e promiscuo, nel testo regolamentare in esame, del termine "*categoria*", che risulta riferito a oggetti e concetti diversi (vi sono già le "*categorie*" di incidenti definite nell'allegato A, le "*categorie*" tipologiche di classificazione delle misure di sicurezza previste nell'allegato B e le "*categorie*" A e B dell'appendice n. 2, che servono a distinguere le misure di sicurezza in base al

termine di adozione e comunicazione). Sarebbe pertanto preferibile usare, in luogo del termine "*categorie*", il termine "*ambiti*" o "*macro-aree*", con riferimento all'elenco suddetto della lettera *b*) del comma 3 della norma primaria.

10. Articolo 10 (*Misure di sicurezza relative alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate*).

Nessuna osservazione

11. Articolo 11 (*Disposizioni finali*).

Nessuna osservazione.

P.Q.M.

Nei sensi suesposti è il parere della Sezione.

L'ESTENSORE
Paolo Carpentieri

IL PRESIDENTE
Paolo Troiano

IL SEGRETARIO
Campobasso Maurizia