RELAZIONE ILLUSTRATIVA

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.

In ragione della rapida evoluzione tecnologica, il rischio che dalle minacce alle reti, ai sistemi informativi e ai servizi informatici, necessari per l'espletamento di funzioni essenziali dello Stato o per la prestazione di servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, possa derivare un pregiudizio per la sicurezza nazionale, ha reso necessario e urgente garantire un livello elevato di sicurezza di tali reti, sistemi informativi e servizi informatici.

Pertanto, con il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 (di seguito indicato "decreto-legge"), è stato istituito il perimetro di sicurezza nazionale cibernetica ed è stato rafforzato il quadro normativo in tema di esercizio dei poteri speciali nei settori di rilevanza strategica.

Il presente schema di provvedimento interviene nel quadro normativo sin qui delineatosi con il decreto-legge e con l'adozione del primo dei provvedimenti di attuazione ivi previsti, e cioè il regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, ai sensi dell'articolo 1, comma 2, del decreto-legge, di recente pubblicazione nella *Gazzetta Ufficiale* n. 261, del 21 ottobre 2020.

Nello specifico, il presente schema di decreto è volto a dare attuazione alle disposizioni di cui all'articolo 1, comma 3, del decreto-legge. Tali disposizioni prevedono che, entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto-legge, con decreto del Presidente del Consiglio dei ministri – adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) – che disciplini, altresì, i relativi termini e le modalità attuative:

a) siano definite le procedure secondo cui i soggetti individuati ai sensi dell'articolo 1, comma 2, lettera *a)*, del decreto-legge, inclusi nell'elenco di cui al comma 2-*bis* del medesimo articolo, notificano al CSIRT italiano gli incidenti aventi impatto sulle reti, sui sistemi informativi e sui servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge. È quindi previsto che il CSIRT italiano inoltri tempestivamente tali notifiche al Dipartimento delle informazioni per la sicurezza (DIS), anche per le attività demandate al Nucleo

per la sicurezza cibernetica, e che il DIS assicuri 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, nell'ipotesi in cui tali notifiche provengano 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, nell'ipotesi in cui le notifiche provengano da un soggetto privato;

b) siano stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge, tenendo conto degli *standard* definiti a livello internazionale e dell'Unione europea. Il decreto-legge definisce, quindi, nove ambiti ai quali le misure stabilite dovranno attenere. Nello specifico, l'articolo 1, comma 3, lettera *b)*, prevede che le misure siano relative:

1) alla struttura organizzativa preposta alla gestione della sicurezza;

1-*bis*) alle politiche di sicurezza e alla gestione del rischio;

2) alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;

3) alla protezione fisica e logica e dei dati;

4) all'integrità delle reti e dei sistemi informativi;

5) alla gestione operativa, ivi compresa la continuità del servizio;

6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

8) 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, di *standard* e di eventuali limiti.

Con riferimento all'elaborazione di tali misure, l'articolo 1, comma 4, del decreto-legge, prevede che vi provvedano, secondo gli ambiti di competenza delineati dallo stesso decreto-legge, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il DIS.

Al fine di assicurare il coordinamento tra il quadro normativo introdotto con l'istituzione del perimetro di sicurezza nazionale cibernetica e le disposizioni già previste, in materia di adozione di misure di sicurezza e obblighi di notifica degli incidenti, da altri plessi dispositivi vigenti (nello specifico, la disciplina di cui al decreto legislativo 18 maggio 2018, n. 65, il c.d. decreto legislativo NIS, nonché quella di cui al decreto legislativo 1° agosto 2003, n. 259, il codice delle comunicazioni elettroniche, e alle correlate disposizioni attuative), l'articolo 1,

comma 8, del decreto-legge, dispone che i soggetti rispettivamente tenuti al rispetto di tali disposizioni:

a) osservino le misure di sicurezza previste dal decreto legislativo NIS, ovvero dal codice delle comunicazioni elettroniche, ove queste siano di livello almeno equivalente a quelle adottate ai sensi dell'articolo 1, comma 3, lettera *b)*, del decreto-legge, e che eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal decreto-legge siano definite – a seconda degli ambiti di rispettiva competenza – dalla Presidenza del Consiglio dei ministri, ovvero dal Ministero dello sviluppo economico avvalendosi anche del Centro di valutazione e certificazione nazionale (CVCN); è quindi previsto che, ove necessario, la Presidenza del Consiglio di ministri e il Ministero dello sviluppo economico si raccordino con le autorità competenti di cui all'art. 7 del decreto legislativo NIS;

b) assolvano l'obbligo di notifica di cui all'articolo 1, comma 3, lettera *a)*, del decreto-legge, disponendo che ciò costituisca anche adempimento degli obblighi rispettivamente previsti dal decreto legislativo NIS, ovvero ai sensi del codice delle comunicazioni elettroniche e delle correlate disposizioni attuative. A tal fine, prevede che, oltre a quanto previsto dall'articolo 1, comma 3, lettera *a)*, del decreto-legge, anche in relazione alle disposizioni di cui all'articolo 16-*ter* del codice delle comunicazioni elettroniche, il CSIRT italiano provveda a inoltrare le notifiche ricevute all'autorità competente di cui all'articolo 7 del decreto legislativo NIS.

È, poi, previsto dall'articolo 1, comma 6, lettera *c)*, del decreto-legge, che le attività di ispezione e verifica, in relazione anche a quanto disposto in materia di notifiche di incidenti e misure di sicurezza, siano svolte dalla Presidenza del Consiglio dei ministri e dal Ministero dello sviluppo economico, per i rispettivi ambiti di competenza definiti dal decreto-legge. È quindi disposto che per le reti, i sistemi informativi e i servizi informatici inclusi nell'elenco di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge – che siano connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato – le attività di ispezione e verifica siano svolte dalle strutture specializzate delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti alla Presidenza del Consiglio dei ministri per i profili di competenza.

Con riguardo alle procedure di adozione e aggiornamento del provvedimento di attuazione dell'articolo 1, comma 3, del decreto-legge, il comma 4-*bis*, del medesimo articolo 1, dispone che lo schema di decreto venga trasmesso alla Camera dei deputati e al Senato della Repubblica, per l'espressione del parere delle Commissioni parlamentari competenti per materia, nonché al Comitato parlamentare per la sicurezza della Repubblica, mentre il successivo comma 5 dispone che all'aggiornamento si proceda secondo le medesime modalità seguite per l'adozione. All'articolo 1, comma 19-*ter*, poi, il decreto-legge dispone che, nei casi in cui sui decreti del Presidente del Consiglio dei ministri previsti dal

medesimo articolo 1 sia acquisito, ai fini della loro adozione, il parere del Consiglio di Stato, i termini ordinatori stabiliti siano sospesi per un periodo di quarantacinque giorni.

Sul punto la relazione tecnica allegata al decreto-legge, positivamente verificata dalla Ragioneria generale dello Stato, chiarisce che per quanto riguarda i soggetti pubblici inclusi nel perimetro, agli oneri derivanti dall'obbligo di attuare le misure di sicurezza si provvederà, a decorrere dagli esercizi finanziari 2020 e 2021, con le risorse finanziarie, umane e strumentali già previste a legislazione vigente.

Al fine di dare attuazione alle previsioni di cui all'articolo 1, commi 3 e 4, del decreto-legge, sono stati adottati appositi moduli organizzativi per la definizione delle procedure di notifica degli incidenti e per l'elaborazione e la condivisione delle misure di sicurezza, anche mediante la costituzione di appositi gruppi di lavoro, che hanno visto la partecipazione dei rappresentanti delle diverse amministrazioni interessate. A conclusione dei lavori, 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 DPCM 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.

Poiché la proposta di decreto ha evidenziato indici che hanno indotto a ritenerne il carattere normativo, si è ritenuto di dover richiedere il parere del Consiglio di Stato, così come avvenuto per il provvedimento di attuazione previsto dall'articolo 1, comma 2, del decreto-legge, in relazione al quale il Supremo Organo consultivo ha convenuto, in sede di parere, sulla sostanza normativa delle disposizioni ivi recate. Al riguardo, è stato considerato, infatti, che il presente decreto del Presidente del Consiglio dei ministri di attuazione delle previsioni di cui all'articolo 1, comma 3, del decreto-legge, appare rivolto a innovare l'ordinamento giuridico, introducendo disposizioni – volte a integrare il precetto delle disposizioni di rango primario – che dettano termini e procedure in materia di obblighi di notifica degli incidenti, nonché l'individuazione delle misure di sicurezza, in relazione ai sopracitati ambiti definiti dal decreto-legge, e i relativi termini e modalità di adozione da parte dei soggetti inclusi nel perimetro. Con particolare riferimento alle misure di sicurezza, il presente decreto provvede a definire il contenuto prescrittivo in relazione agli ambiti delineati dal legislatore, stabilendo quali siano le specifiche misure che i soggetti tenuti alla loro osservanza dovranno adottare, quali siano le modalità di attuazione delle disposizioni introdotte e quali i termini entro cui provvedere.

Sullo schema di decreto del Presidente del Consiglio dei ministri è, quindi, intervenuto il CISR – organo al quale spetta, in ossequio alla richiamata procedura,

la proposta di adozione – che, ai fini della trasmissione al Consiglio di Stato, ha favorevolmente deliberato sul testo, in via preliminare, nella seduta del 27 ottobre 2020.

Tanto premesso, si illustra di seguito il contenuto del decreto e delle singole disposizioni con le quali si dà attuazione alle prescrizioni indicate dal decreto-legge.

Il presente decreto si compone di 11 articoli suddivisi in IV capi, di cui il capo I 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, ed è integrato, in ragione della complessità e del livello tecnico della disciplina, da 3 allegati, di cui il primo (allegato A), previsto dall'articolo 2, recante due tabelle di classificazione degli incidenti aventi impatto sui beni ICT (nel significato che verrà di seguito specificato in sede di illustrazione dell'articolo 1), il secondo (allegato B), previsto dall'articolo 7, recante le misure di sicurezza, e il terzo (allegato C), previsto dall'articolo 9, recante misure minime per la tutela delle informazioni.

L'**articolo 1**, del capo I, è dedicato alle definizioni. Nello specifico, nell'ottica di garantire la coerenza con l'assetto definitorio delineato dagli altri provvedimenti di attuazione del decreto-legge (il richiamato regolamento adottato in attuazione dell'articolo 1, comma 2, del decreto-legge, con DPCM n. 131 del 2020, e lo schema di regolamento da adottare con DPR, in attuazione del comma 6 del medesimo articolo 1 del decreto-legge, sul quale è stato reso il parere del Consiglio di Stato - Sezione consultiva per gli atti normativi, nell'adunanza del 20 ottobre u.s.), l'articolo 1 reca soltanto quelle definizioni 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 presente decreto, significati tecnici specifici. Si evidenziano, in particolare, le definizioni di:

- "*soggetti inclusi nel perimetro*", con cui si intende fare riferimento ai soggetti che siano stati individuati secondo le procedure di cui all'articolo 1, comma 2, lettera *a)*, del decreto-legge, e inclusi nell'elencazione contenuta nell'atto amministrativo adottato ai sensi dell'articolo 1, comma 2-*bis*, del decreto-legge;
- "*bene ICT*", conforme alla definizione, già recata dal DPCM n. 131 del 2020, che è stata adeguata al fine di tenere conto, in ragione dell'avanzamento del processo di attuazione del perimetro di sicurezza nazionale cibernetica, dell'inserimento, da parte di ciascuno dei soggetti inclusi nel perimetro, dei beni ICT nell'elenco di cui all'articolo 1, comma 2, lettera *b*), del decreto-legge, che costituisce un antecedente logico rispetto all'ambito normativo di cui al presente decreto;
- "*impatto sul bene ICT*", con cui, infine, si è provveduto a specificare, avuto riguardo a un bene ICT, cosa debba intendersi per "*impatto*", atteso che la nozione comune di "*impatto*" fa riferimento ai concetti di "*urto*", che poco sembra attagliarsi alla realtà cibernetica, o di "*evento*", di portata semantica

molto ampia. È stato così individuato e specificato, in assenza di disposizioni definitorie nel provvedimento legislativo d'urgenza, l'ambito di operatività della disposizione di cui all'articolo 1, comma 3, lettera *a)*, del decreto-legge, 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)". La formulazione della definizione ha trovato ancoraggio al concetto di "*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*", già formulato nell'ambito dell'articolo 7, comma 2, lettera *a)*, numero 1), del richiamato regolamento adottato con DPCM n. 131 del 2020.

Al fine di giungere, pertanto, a delineare il significato, in sede di normativa di attuazione, del concetto di "*incidenti aventi impatto su beni ICT*" recato dalla disposizione di rango primario, infine, si è ritenuto di non doversi discostare dalla definizione di "*incidente*", già adottata nell'ambito del quadro attuativo delle disposizioni del decreto-legge, come sin qui delineatosi con i provvedimenti previsti dall'articolo 1, commi 2 e 6, che è stata, pertanto, riproposta.

L'**articolo 2** apre il capo II dedicato alle notifiche di incidente. Nello specifico, avuto anche riguardo alle prassi e agli *standard* definiti a livello internazionale e dell'Unione europea, sono stati classificati, in due tabelle riportate in allegato A al presente decreto, quegli incidenti per i quali il decreto-legge pone l'obbligo di notifica in capo ai soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge (nelle definizioni di cui all'articolo 1 indicati quali "*soggetti inclusi nel perimetro*"), e cioè gli incidenti aventi impatto sui beni ICT. In ossequio alla definizione di incidente recata dal regolamento adottato con DPCM n. 131 del 2020, la tassonomia degli incidenti risponde all'esigenza di strutturare un approccio che ne ricomprenda una casistica ampia, indipendentemente dall'intenzionalità o dall'accidentalità che li possa caratterizzare. Pertanto, si è provveduto a unificare due modelli largamente impiegati dalle comunità internazionali, scientifica e di sicurezza informatica, traendo spunto, al contempo, da standard *de facto* e da migliori pratiche anche internazionali. La suddivisione nelle due tabelle è stata operata a seconda della gravità degli incidenti, recando i meno gravi nella prima e i più gravi nella seconda, anche tenuto conto della tempistica necessaria per una risposta efficace. Per quanto concerne la tabella n. 1, vi si trovano elencate, in particolare, le tipologie di incidenti che si possono configurare come precursori rispetto a ulteriori incidenti idonei, a loro volta, a determinare un impatto ancora più significativo sui beni ICT. Tale ultima tipologia di incidenti è stata inclusa nella tabella n. 2. A tale suddivisione corrisponde, come verrà di seguito meglio illustrato nell'ambito dell'articolo 3, una diversa definizione dei termini per l'adempimento dell'obbligo di notifica: sei ore per quelli della tabella n. 1 e un'ora per quelli della tabella n. 2. La scelta di indicare un termine più breve e stringente (un'ora) per gli incidenti di cui alla tabella n. 2 è legata alla necessità di assicurare tempi più rapidi di reazione da parte dell'intera architettura nazionale *cyber* per gli incidenti più gravi, anche in ragione della portata degli impatti discendenti.

L'**articolo 3** delinea le procedure e definisce i termini per la notifica al CSIRT italiano – istituito presso il DIS ai sensi dell'articolo 8, comma 1, del decreto legislativo 18 maggio 2018, n. 65 (c.d. decreto legislativo NIS) – degli incidenti aventi impatto su un bene ICT, e cioè di uno degli incidenti classificati nelle tabelle in allegato A al presente decreto. La disposizione chiarisce, altresì, che deve essere notificato uno degli incidenti di cui all'allegato A, che, in aderenza al dettato legislativo, abbia comunque impatto su un bene ICT, anche nell'ipotesi in cui l'incidente si verifichi a carico di un sistema informativo, o di un servizio informatico, o parti di essi, che, anche in esito all'analisi del rischio di cui all'articolo 7, comma 2, del regolamento adottato con DPCM n. 131 del 2020, condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero *software* di base quali sistemi operativi e di virtualizzazione.

Per l'effettuazione della notifica, vengono individuati i canali di comunicazione del CSIRT italiano, prescrivendo, per ragioni di coerenza ordinamentale, che gli stessi abbiano i requisiti di cui al punto 1, lettera *a)*, dell'allegato I, del decreto legislativo NIS, secondo modalità definite dal CSIRT italiano e rese disponibili sul sito Internet di tale organo.

Vengono, quindi, indicati i termini entro i quali adempiere all'obbligo di notifica: entro sei ore per gli incidenti classificati in tabella n. 1 ed entro un'ora per gli incidenti classificati in tabella n. 2. La definizione dei termini di notifica, di cui il più breve fissato in un'ora, è stata determinata a valle di una ricognizione dei termini di notifica esistenti in altri settori, come, in particolare, quello della sicurezza delle reti e dei sistemi informativi di cui al decreto legislativo NIS, ovvero quello della protezione dei dati personali di cui al Regolamento generale sulla protezione dei dati personali dell'UE (il "GDPR"), nonché quello relativo ai servizi di pagamento nel mercato interno disciplinato dalla direttiva (UE) 2015/2366. Sono stati tenuti in considerazione, quindi, lo specifico ambito in cui operano le disposizioni del decreto-legge, e cioè quello della sicurezza nazionale cibernetica, e l'essenzialità del fattore temporale ai fini di un rapido intervento in caso di incidente.

Per ciò che riguarda il momento iniziale dal quale decorre il termine per l'adempimento dell'obbligo di notifica, esso è stato individuato nel momento in cui il soggetto incluso nel perimetro, titolare del bene ICT impattato dall'incidente, "*ne è venuto a conoscenza*". Tale soluzione, la cui formulazione è stata mutuata dalla disciplina in materia di protezione dei dati personali e di notifica dei c.d. *data breach*, è volta, da un lato, a dare atto della peculiarità degli incidenti informatici, la cui scoperta può avvenire, successivamente, anche a distanza di molto tempo; dall'altro, a consentire ai soggetti titolari dei beni ICT di poter effettuare la notifica nei termini previsti all'esito di un processo di "*triage*", finalizzato alla verifica preliminare in ordine alla circostanza che l'incidente verificatosi presenti gli elementi essenziali contenuti nelle fattispecie di incidente classificate in allegato A.

Successivamente al momento iniziale della notifica, anche in considerazione dei brevi termini fissati, è previsto che il soggetto debba provvedere a una tempestiva

integrazione della notifica stessa, qualora venga a conoscenza di nuovi elementi significativi di natura tecnica o comunque correlati all'incidente oggetto di notifica (comma 4). È, infine, prevista la possibilità per il CSIRT italiano di richiedere al soggetto notificante sia elementi di aggiornamento sull'incidente in corso (comma 6), sia, nella fase di risoluzione dell'incidente (individuata nel momento in cui siano stati definiti ed avviati da parte del soggetto notificante i piani di attuazione delle attività per il ripristino dei beni ICT impattati dall'incidente), la trasmissione di una relazione tecnica che dia conto degli elementi significativi dell'incidente e, in particolare, delle conseguenze dell'impatto sui beni ICT e delle azioni intraprese per porvi rimedio (comma 7).

Al fine di coordinare gli obblighi del soggetto incluso nel perimetro relativi alle notifiche di incidente, previsti dal decreto-legge, con le eventuali esigenze di segretezza investigativa, discendenti dall'avvio di indagini da parte dell'autorità giudiziaria, viene previsto che il soggetto notificante proceda all'integrazione della notifica (comma 4), fornisca su richiesta del CSIRT italiano elementi di aggiornamento (comma 6), e trasmetta la relazione tecnica che illustra gli elementi significativi dell'incidente al CSIRT italiano (comma 7), salvo che l'autorità giudiziaria procedente non abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

Con riferimento, infine, al comma 5, allo scopo di dare attuazione alle disposizioni di cui all'articolo 1, comma 8, lettera *b)*, del decreto-legge, sono previsti gli opportuni raccordi per l'assolvimento degli obblighi di notifica previsti dalla disciplina di cui al decreto legislativo NIS e al codice delle comunicazioni elettroniche (e correlate disposizioni attuative). In particolare, è stabilito che la notifica di incidente effettuata nell'ambito della disciplina introdotta dal decreto-legge valga anche ai fini dell'adempimento dell'obbligo di notifica previsto dal codice delle comunicazioni elettroniche e dal decreto legislativo NIS. In tale ipotesi, i soggetti interessati, qualora l'incidente rilevi anche ai fini del decreto legislativo NIS, ovvero del codice delle comunicazioni elettroniche, nell'effettuare la notifica al CSIRT italiano, indicano, rispettivamente, l'autorità competente NIS (alla quale il CSIRT italiano provvederà ad inoltrare la notifica), ovvero che la medesima notifica costituisce anche adempimento dell'obbligo previsto dalla disciplina di cui al codice delle comunicazioni elettroniche e correlate disposizioni attuative. In via ricognitiva, poi, viene precisato che restano fermi gli obblighi di notifica, secondo le relative procedure, previsti dal decreto legislativo NIS e dal codice delle comunicazioni elettroniche e relative disposizioni attuative per quegli incidenti che non rientrano nell'ambito di applicazione del decreto-legge.

L'**articolo 4** è volto a disciplinare la possibilità per i soggetti inclusi nel perimetro di notificare incidenti non rientranti tra le categorie per le quali è prevista la notifica obbligatoria. Con tale disposizione in materia di notifiche volontarie, che in parte recepisce analogo istituto previsto nell'ambito del decreto legislativo NIS, si intende poter consentire, da un lato, ai soggetti, di comunicare incidenti che ritengano comunque significativi e meritevoli di essere portati all'attenzione del

CSIRT italiano, dall'altro, allo stesso CSIRT italiano, di ampliare il quadro conoscitivo e statistico relativo alle tipologie di incidenti che occorrono a danno delle reti, dei sistemi informativi e dei servizi informatici dei soggetti inclusi nel perimetro. Ciò, anche in aderenza ai compiti assegnati al CSIRT italiano dal decreto legislativo NIS (articolo 8 e allegato I, punto 2), tra i quali rientrano il monitoraggio degli incidenti a livello nazionale e l'analisi dinamica dei rischi e degli incidenti.

L'**articolo 5** è dedicato, in ossequio alle previsioni di cui all'articolo 1, commi 3, lettera *a)*, e 8, lettera *b)*, del decreto-legge, alla trasmissione delle notifiche ricevute dal CSIRT italiano ai diversi soggetti istituzionali destinati a riceverle. È inoltre prevista la possibilità di stipulare apposite intese con ciascuna delle amministrazioni interessate, al fine di concordare le modalità di trasmissione delle notifiche. Tenuto conto che, per le attività di ispezione e verifica relative, in particolare, ai beni ICT connessi alla difesa e sicurezza militare dello Stato, sono competenti, ai sensi dell'articolo 1, comma 6, lettera *c)*, terzo periodo, del decreto-legge, le strutture specializzate del Ministero della difesa, la possibilità di stipulare apposite intese è stata estesa anche in relazione a quell'amministrazione in merito alle notifiche di incidente che la stessa provvede a effettuare.

L'**articolo 6** reca disposizioni di carattere ricognitivo. In ragione dell'esclusione dall'elenco dei beni ICT per le reti, per i sistemi informativi e per i servizi informatici attinenti alla gestione delle informazioni classificate, disposta dall'articolo 1, comma 2, lettera *b*), del decreto-legge, viene confermato, per ragioni di chiarezza ordinamentale, che i relativi incidenti non soggiacciano all'obbligo di notifica di cui al presente decreto. È confermato, quindi, che per tali incidenti resta fermo quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, e dalle correlate disposizioni attuative.

L'**articolo 7** apre il capo III dedicato alle misure volte a garantire elevati livelli di sicurezza dei beni ICT. Le misure di carattere tecnico e organizzativo stabilite con il presente decreto, riportate sistematicamente nell'allegato B, integrano di contenuto normativo i richiamati ambiti delineati dal legislatore primario nelle disposizioni di cui all'articolo 1, comma 3, lettera *b)*, del decreto-legge (tra questi, a titolo esemplificativo, si evidenziano 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 l'individuazione delle misure, è stato assunto, quale base di riferimento, il "*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). Tale

strumento scientifico ampiamente riconosciuto a livello nazionale è stato, quindi, adeguato allo specifico contesto operativo delineato dal perimetro di sicurezza nazionale cibernetica. A tale riguardo, giova evidenziare che il *Framework* nazionale, da un lato, ha rappresentato, sin dal 2015, uno strumento elaborato in condivisione tra realtà istituzionali e soggetti privati, pubblicamente disponibile con la finalità di promuovere un approccio volontario e omogeneo per affrontare la cybersicurezza, al fine di ridurre il rischio legato alla minaccia nell'ambito cyber; dall'altro, è stato assunto, anche nell'ambito della disciplina di recepimento della direttiva NIS, quale base di riferimento da parte delle autorità competenti NIS per l'adozione delle linee guida sulle misure di sicurezza di cui gli operatori di servizi essenziali (OSE) devono tener conto ai sensi di quella normativa. Il *Framework* nazionale, peraltro, fa a sua volta riferimento ad altri autorevoli strumenti internazionali in materia, quali, in particolare, il *Framework for Improving Critical Infrastructure Cybersecurity* del National Institute of Standards and Technology (NIST).

La scelta di adottare, quale base di riferimento, il *Framework* nazionale ha anche consentito di realizzare un opportuno punto di equilibrio tra il livello prescrittivo, come definito dal legislatore regolamentare, e quello della concreta applicazione delle diverse misure, che viene demandato a ciascun soggetto nell'ambito della rispettiva realtà organizzativa. In tal senso, infatti, il presente decreto, con le misure di sicurezza che ha provveduto a individuare, intende prescrivere ai soggetti obblighi di natura tecnica e organizzativa e fornire, per ciascuna di esse, una specifica più dettagliata dell'implementazione minima attesa, nonché delle modalità richieste al fine di descriverne l'adozione e dimostrarne l'attuazione. Allo stesso tempo, la scelta sulle modalità di attuazione delle misure viene necessariamente rimessa alle valutazioni di ciascun soggetto incluso nel perimetro – in relazione alle proprie specifiche caratteristiche tecniche e organizzative – che avverranno anche a seguito delle analisi del rischio che condurrà ciascun soggetto incluso nel perimetro, tra cui quella già prevista, ai fini dell'individuazione dei beni ICT, dal regolamento adottato con DPCM n. 131 del 2020.

Le misure sono state organizzate sistematicamente nell'allegato B 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. Ciò al fine di consentire un più immediato riferimento e ausilio alla lettura e all'applicazione delle misure in parola.

Le misure di cui all'allegato B sono caratterizzate dalla misurabilità. Nello specifico, anche al fine di poter agevolare lo svolgimento delle attività di verifica e ispettive, ogni sottocategoria dà luogo alla produzione di un'evidenza documentale o fisica, immediatamente apprezzabile e valutabile. A titolo esemplificativo, si considerino: il "*documento aggiornato che descrive i processi di gestione del rischio include la parte relativa ai rischi legati alla cybersecurity*" di cui alla sottocategoria 2.2.2 (ID.GV-4), il "*piano aggiornato di verifica e test di sicurezza*

che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica dei beni ICT e dell'efficacia delle misure di sicurezza tecniche e procedurali" di cui alla sottocategoria 2.3.1 (ID.RA-1), ovvero ancora la "*pianificazione aggiornata degli audit di sicurezza previsti*" e il "*registro degli audit di sicurezza effettuati con la relativa documentazione*" previsti nell'ambito della sottocategoria 3.1.1. (PR.AC-1).

Le misure di sicurezza individuate dal presente decreto corrispondono ai nove ambiti delineati dal decreto-legge all'articolo 1, comma 3, lettera *b)*. 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.

Al fine del completamento del quadro di protezione dei "beni ICT" infine, sono indicate, ai punti 2.1.2 (ID.AM-2) e 2.5.2 (ID.SC-2) del richiamato allegato B, previsioni di contenuto esortativo, chiaramente introdotte con la formula "*si raccomanda*", le cui determinazioni in merito a una loro attuazione sono demandate a ciascun soggetto incluso nel perimetro.

L'**articolo 8** è dedicato alla definizione delle modalità con le quali i soggetti inclusi nel perimetro debbano adottare, per ciascun bene ICT di rispettiva pertinenza, le misure di cui all'allegato B, nonché dei relativi termini entro i quali provvedere. In particolare, sono previsti due differenti termini di adozione delle misure, sei mesi e ventiquattro mesi, distinti a seconda che si tratti di misure, rispettivamente, di più immediata attuazione, ovvero per la cui implementazione siano necessari interventi che richiedano, potenzialmente, una più impegnativa attività sotto i profili progettuali e programmatici. In ragione di tale distinzione, le misure individuate nell'allegato B sono state suddivise in due macro-categorie, categoria A (da adottare entro 6 mesi) e categoria B (da adottare entro 24 mesi), e di tale classificazione, per pronto e chiaro riferimento dei soggetti tenuti all'adozione delle misure nei diversi tempi previsti, è stato dato atto in un'apposita tabella (in appendice n. 2 all'allegato B).

Per l'individuazione del momento iniziale dal quale far decorrere il termine entro il quale adottare le misure di sicurezza, si è dovuto necessariamente tenere conto del quadro dispositivo delineato dall'articolo 1, comma 2, del decreto-legge e dal regolamento adottato con DPCM n. 131 del 2020 adottato in sua attuazione. In capo ai soggetti inclusi nel perimetro, infatti, è previsto l'obbligo, in particolare, di predisporre l'elenco dei beni ICT di rispettiva pertinenza e di trasmettere tale elenco entro sei mesi dalla data in cui è avvenuta la comunicazione di inclusione nel perimetro di sicurezza nazionale cibernetica. La predisposizione dell'elenco dei

beni ICT che, come già sopra anticipato, avviene, da parte di ciascun soggetto incluso nel perimetro, in esito all'effettuazione di un'analisi del rischio per ogni funzione essenziale dello Stato esercitata o servizio essenziale prestato, rappresenta, pertanto, un presupposto logico e di fatto per l'adozione delle misure di sicurezza per ciascuno dei beni ICT individuati nel predetto elenco. Conseguentemente, è stato stabilito che le misure di categoria A e B debbano essere adottate, rispettivamente, entro sei e ventiquattro mesi, dalla data di trasmissione (mediante la piattaforma digitale costituita presso il DIS ai sensi dell'articolo 9 del DPCM n. 131/2020) degli elenchi dei beni ICT. Infine, non essendo possibile conoscere a priori le tempistiche di adozione, ai sensi dell'articolo 1, comma 2-*bis*, del decreto-legge, dell'atto amministrativo recante l'elencazione dei soggetti inclusi nel perimetro, né la data in cui ciascuno di tali soggetti provvederà a trasmettere l'elenco dei beni ICT di rispettiva pertinenza, è stato previsto che, qualora la trasmissione dell'elenco dei beni ICT avvenga in una data antecedente a quella dell'entrata in vigore del presente decreto, i termini decorreranno da tale ultima data.

È quindi previsto che i soggetti tenuti comunichino, mediante la predetta piattaforma digitale costituita presso il DIS, le modalità con le quali hanno provveduto ad adottare le misure di sicurezza. A tal fine, è previsto l'utilizzo di un apposito modulo che verrà reso disponibile dal DIS.

Ai fini dello svolgimento delle attività di ispezione e verifica da parte dei soggetti individuati ai sensi dell'articolo 1, comma 6, lettera *c)*, primo periodo, del decreto-legge (Presidenza del Consiglio dei ministri e Ministero dello sviluppo economico), è previsto che il DIS renda loro tempestivamente disponibili le comunicazioni ricevute da parte dei soggetti inclusi nel perimetro, relative alle modalità di adozione e agli eventuali aggiornamenti delle misure di sicurezza. Infine, poiché il decreto-legge prevede che le attività di ispezione e verifica per i beni ICT connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, siano svolte dalle competenti strutture delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate, è escluso che le comunicazioni sulle misure di sicurezza concernenti tali beni ICT vengano, successivamente alla loro trasmissione e conservazione sulla piattaforma digitale costituita presso il DIS, rese disponibili alle strutture della Presidenza del Consiglio dei ministri e del Ministero dello sviluppo economico.

L'**articolo 9** individua, nell'allegato C al presente decreto, misure minime di sicurezza di natura tecnica e organizzativa volte a tutelare le informazioni relative all'elenco dei soggetti inclusi nel perimetro, all'elenco dei beni ICT, agli elementi delle notifiche di incidente, al modello di cui all'articolo 8 recante le modalità di adozione delle misure di sicurezza e, infine, alla documentazione relativa alle misure di sicurezza adottate da parte dei soggetti inclusi nel perimetro ai sensi degli articoli 7 e 8. Ciò, anche al fine di corrispondere all'esigenza di tutela delle informazioni emersa in sede di adozione del regolamento di cui al DPCM n. 131

del 2020. In quella sede, infatti, è stato previsto (articolo 10 del richiamato regolamento), nelle more dell'adozione del presente decreto, che l'elencazione dei soggetti inclusi nel perimetro e gli elenchi dei beni ICT, comprensivi della descrizione dell'architettura e componentistica, nonché dell'analisi del rischio, fossero trattati, conservati e trasmessi con modalità idonee a garantirne la sicurezza, mediante misure tecniche e organizzative adeguate, fatta salva l'eventuale attribuzione di classifiche di segretezza ai sensi dell'articolo 42 della legge n. 124 del 2007.

A tali tipologie di informazioni sono state altresì aggiunte quelle attinenti alle notifiche effettuante ai sensi dell'articolo 3, al modello di cui all'articolo 8 e alla documentazione relativa alle misure di sicurezza di cui all'allegato B, adottate ai sensi degli articoli 7 e 8.

Le misure sono state suddivise in due macro-categorie, la prima relativa ai trattamenti svolti con l'ausilio di strumenti elettronici, la seconda relativa a misure di sicurezza fisica e documentale e rientrano nell'ambito delle categorie di cui all'articolo 1, comma 3, lettera *b)*, numeri 3 e 4, del decreto-legge, relative alla protezione fisica e logica e dei dati (numero 3) e all'integrità delle reti e dei sistemi informativi (numero 4).

Per tali misure – che definiscono un livello minimo di tutela delle informazioni – sono previsti termini più brevi di adozione rispetto a quelli previsti per le misure di sicurezza di cui all'allegato B. Nello specifico, in ragione della necessità di garantire in tempi rapidi la tutela delle predette informazioni, che dovranno essere trattate fin dalla fase iniziale dell'operatività delle misure attuative del decreto-legge, e tenuto conto della tipologia di misure prescritte, che non richiedono particolari interventi da parte dei soggetti tenuti al loro rispetto, è previsto che le stesse debbano essere applicate entro sessanta giorni dalla data di entrata in vigore del presente decreto. È, inoltre, precisato che resta ferma l'adozione da parte dei soggetti inclusi nel perimetro dell'ulteriore e più elevato livello di sicurezza delle misure di cui all'allegato B.

Infine, fermo restando quanto previsto dagli articoli 6 e 10, in relazione alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate, in via ricognitiva, viene chiarito che, nel caso in cui alle informazioni, relative a uno degli ambiti oggetto dell'applicazione delle misure minime di cui all'allegato C, venga attribuita una classifica di segretezza ai sensi dell'articolo 42 della legge n. 124 del 2007, troverà applicazione la disciplina recata dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, e dalle correlate disposizioni attuative.

L'**articolo 10**, per le stesse ragioni di cui all'articolo 6, e in particolare in ragione dell'esclusione dall'elenco dei beni ICT delle reti, dei sistemi informativi e dei servizi informatici attinenti alla gestione delle informazioni classificate disposta dall'articolo 1, comma 2, lettera *b*), del decreto-legge, per ragioni di chiarezza ordinamentale, viene precisato in via ricognitiva, che a tali reti, sistemi informativi

e servizi informatici non si applicano le misure di sicurezza previste dal presente decreto. Viene, quindi, confermato, anche in tale ambito, che resta fermo quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007 e dalle correlate disposizioni attuative.

L'**articolo 11**, infine, in aderenza al vincolo di spesa posto dal legislatore, indica che dal presente decreto non derivano nuovi o maggiori oneri per la finanza pubblica.

Per l'illustrazione dei contenuti degli allegati A, B e C, si rinvia a quanto illustrato nell'ambito, rispettivamente, degli articoli 2, 7 e 9.

RELAZIONE TECNICA

Il decreto-legge 21 settembre 2019, n.105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante "disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica", ha istituito il perimetro di sicurezza nazionale cibernetica al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici dei soggetti pubblici e degli operatori economici privati che espletano funzioni essenziali per lo Stato o che prestano servizi essenziali 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. Con il medesimo decreto-legge, inoltre, sono state introdotte disposizioni volte a rafforzare il quadro normativo in tema di esercizio dei poteri speciali nei settori di rilevanza strategica.

Il presente decreto del Presidente del Consiglio dei ministri interviene nel quadro normativo sin qui delineatosi con il decreto-legge e con l'adozione del primo dei provvedimenti di attuazione ivi previsti, e cioè il regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, ed è adottato in attuazione dell'articolo 1, comma 3, del decreto-legge, su proposta del CISR.

Nello specifico, il presente decreto disciplina, regolandone, altresì, i relativi termini e le modalità attuative:

- ai sensi dell'articolo 1, comma 3, lettera *a*), le procedure con cui i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, individuati nell'atto amministrativo di cui all'articolo 1, comma 2-*bis*, del decreto-legge, notificano al CSIRT italiano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici inclusi nell'elenco di cui all'articolo 1, comma 2, lettera *b*) del decreto-legge (nelle definizioni del presente decreto indicati come "beni ICT");
- ai sensi dell'articolo 1, comma 3, lettera *b*), le misure volte a garantire elevati livelli di sicurezza dei beni ICT, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

In relazione a tanto, il presente decreto prevede due tipologie di obblighi che, come si illustrerà, non comportano nuovi o maggiori oneri per la finanza pubblica: obblighi di notifica e obblighi di adozione delle misure di sicurezza.

In particolare, per quanto concerne gli obblighi di notifica, il decreto impone di notificare, tramite appositi canali di comunicazione del CSIRT italiano, gli incidenti che abbiano impatto su un bene ICT. 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. Prescrive, inoltre, un dovere di integrazione della notifica nel caso in cui il soggetto incluso nel perimetro venga a conoscenza di nuovi elementi significativi.

All'adempimento dei suddetti obblighi di notifica, i soggetti pubblici inclusi nel perimetro provvedono nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente.

Con riferimento alla seconda tipologia di obblighi, il decreto dispone che i soggetti inclusi nel perimetro, adottino, per ciascun bene ICT di rispettiva pertinenza, le misure di sicurezza individuate nell'allegato B al presente decreto e corrispondenti agli ambiti indicati all'articolo 1, comma 3, lettera *b*), del decreto-legge, comunicandone l'avvenuta adozione e le relative modalità mediante il modello reso disponibile dal DIS tramite gli appositi canali di comunicazione del CSIRT italiano. È inoltre previsto che i soggetti tenuti all'adozione delle misure di sicurezza debbano adeguare le stesse ogniqualvolta dovessero ritenerlo necessario a seguito di aggiornamenti occorsi sull'elenco dei beni ICT.

In relazione a tali oneri, si provvederà, come è stato precisato anche nella relazione tecnica allegata al decreto-legge, positivamente verificata dalla Ragioneria Generale dello Stato, a decorrere dagli esercizi finanziari 2020/2021, con le risorse finanziarie, umane e strumentali disponibili a legislazione vigente.

Per quanto concerne la mancanza di impatto sulla finanza pubblica in ordine all'eventuale adeguamento alle misure di sicurezza, si richiama l'articolo 1, comma 18, del decreto-legge, il quale precisa, infatti, che gli eventuali adeguamenti alle prescrizioni di sicurezza sono effettuati con le risorse finanziarie disponibili a legislazione vigente.

Sia in relazione alla modalità di trasmissione delle notifiche di incidente, che in riferimento allo strumento da utilizzare per la comunicazione in ordine all'avvenuta adozione delle misure di sicurezza e dei relativi aggiornamenti, il decreto prevede che vengano utilizzati gli appositi canali di comunicazione del CSIRT italiano.

In primo luogo, è previsto che la notifica avvenga tramite appositi canali di comunicazione del CSIRT italiano aventi i requisiti di cui al punto 1, lettera a), dell'allegato I, del decreto legislativo 18 maggio 2018 n. 65, secondo le modalità definite dal CSIRT italiano e rese disponibili sul sito Internet dello stesso CSIRT italiano, già reso operativo. Il ricorso a tali canali di comunicazione, in quanto relativi al CSIRT italiano, già istituito presso il DIS con il decreto legislativo n. 65 del 2018 e successivamente disciplinato con il decreto del Presidente del Consiglio dei ministri 8

agosto 2019, non comporta nuovi oneri o maggiori per la finanza pubblica, atteso che all'implementazione dei suddetti canali si provvederà con le risorse finanziarie, umane e strumentali previste nei pertinenti capitoli del bilancio del DIS, dell'AISE e dell'AISI di cui all'articolo 29 della legge 3 agosto 2007, n. 124, già disponibili.

In secondo luogo, è previsto che l'avvenuta adozione delle misure di sicurezza, comprensiva delle relative modalità, venga comunicata dal soggetto incluso nel perimetro mediante la piattaforma digitale costituita presso il DIS, ai sensi del regolamento adottato con il DPCM n. 131 del 2020, con il modello reso disponibile dal DIS tramite gli appositi canali di comunicazione del CSIRT italiano. L'utilizzo della piattaforma digitale, come indicato nella relazione tecnica al citato regolamento adottato con DPCM n. 131 del 2020, non comporta nuovi oneri a carico della finanza pubblica, poiché al funzionamento della piattaforma istituita presso il DIS, si provvede con le risorse finanziarie, umane e strumentali previste nei pertinenti capitoli del bilancio del DIS, dell'AISE e dell'AISI di cui al citato articolo 29 della legge 3 agosto 2007, n. 124, già disponibili. Per quanto concerne l'utilizzo del modello reso disponibile dal DIS tramite gli appositi canali di comunicazione del CSIRT italiano, alla luce delle argomentazioni sopra riportate, non si ravvisa un impatto sulla finanza pubblica.

Sempre in relazione agli obblighi di adozione delle misure di sicurezza, il presente decreto individua, infine, misure di sicurezza minime, di natura tecnica e organizzativa, che i soggetti inclusi nel perimetro sono tenuti ad applicare per tutelare le informazioni relative: all'elencazione dei soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge; all'elenco dei beni ICT di cui all' all'articolo 1, comma 2, lettera *b*), del decreto-legge; agli elementi delle notifiche di incidente, di cui all'articolo 3 del presente decreto; al modello, infine, con cui viene comunicata l'adozione, e le relative modalità, delle misure di sicurezza da applicarsi sui beni ICT, di cui all'articolo 8 del presente decreto. Anche in relazione a tali oneri, si provvederà, a decorrere dagli esercizi finanziari 2020/2021, con le risorse finanziarie, umane e strumentali disponibili a legislazione vigente, così come sopra precisato con riferimento agli oneri derivanti dall'adozione delle misure di sicurezza sui beni ICT.

ANALISI TECNICO-NORMATIVA

Titolo: 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.

Amministrazione referente: Presidenza del Consiglio dei ministri.

PARTE I - ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1) Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di governo.

Il decreto del Presidente del Consiglio dei ministri è adottato 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, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica (nel prosieguo "decreto-legge").

Nello specifico, nel provvedere a regolare, altresì, i relativi termini e le modalità attuative, lo schema di decreto:

- disciplina, ai sensi dell'articolo 1, comma 3, lettera *a*), del decreto-legge, le procedure con cui i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, individuati nell'atto amministrativo di cui all'articolo 1, comma 2-*bis*, del decreto-legge, notificano al CSIRT italiano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici inclusi nell'elenco di cui all'articolo 1, comma 2, lettera *b*), del decreto-legge (nelle definizioni del presente decreto indicati come "beni ICT");
- stabilisce, ai sensi dell'articolo 1, comma 3, lettera *b*), del decreto-legge, le misure volte a garantire elevati livelli di sicurezza dei beni ICT, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

Il presente schema di decreto è adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica, sulla base della procedura prevista all'articolo 1, commi 3 e 4-*bis,* del decreto-legge, che dispone la previa trasmissione del testo alla Camera dei deputati e al Senato della Repubblica per l'espressione del parere delle Commissioni parlamentari competenti per materia, nonché al Comitato parlamentare per la sicurezza della Repubblica. Poiché la proposta di decreto ha evidenziato indici che hanno indotto a ritenerne il carattere normativo, lo schema viene inoltre sottoposto al parere del Consiglio di Stato.

Il presente decreto, ai sensi dell'articolo 1, comma 5, del decreto-legge, è inoltre soggetto ad aggiornamento periodico, con cadenza almeno biennale, con le medesime modalità seguite per la sua adozione.

Trattandosi di intervento attuativo del decreto-legge, l'adozione del presente decreto risulta necessaria al fine di assicurare la concreta operatività degli obblighi di notifica e di adozione delle misure di sicurezza sottesi all'istituzione del perimetro di sicurezza nazionale cibernetica ed è coerente con l'impegno del Governo di adottare, accanto alle azioni dirette ad accrescere la digitalizzazione del Paese – fattore imprescindibile di sviluppo e di crescita – tutte le misure necessarie per assicurare elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale.

2) Analisi del quadro normativo nazionale.

Il presente decreto attuativo si innesta nel quadro normativo sin qui delineatosi con il decreto-legge in tema di sicurezza nazionale cibernetica e con l'adozione del primo dei provvedimenti di attuazione ivi previsti, e cioè il regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, disciplinando, pertanto, nella prospettiva della tutela della sicurezza nazionale, le misure necessarie ad assicurare elevati livelli di sicurezza informatica di reti, sistemi informativi e servizi informatici 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 o interruzione, anche parziali, ovvero utilizzo improprio, possano derivare pregiudizi per la sicurezza nazionale.

Vengono, a tal fine, definite le procedure per la notifica degli incidenti aventi impatto sui beni ICT, e individuate le misure di sicurezza da applicarsi sui beni ICT.

Nello specifico, il quadro normativo in cui interviene il presente decreto di attuazione è delineato dai seguenti provvedimenti:

- la legge 3 agosto 2007, n. 124, recante l'istituzione del Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto, che all'articolo 1, comma 3-*bis,* dispone che il Presidente del Consiglio dei ministri impartisce al Dipartimento delle informazioni per la sicurezza (DIS) e ai Servizi di informazione per la sicurezza direttive per rafforzare la protezione cibernetica e la sicurezza informatica nazionali e all'articolo 4, comma 3, lettera d-*bis*), attribuisce al DIS il compito di coordinare le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;
- il decreto legislativo 15 settembre 2003, n. 259 (di seguito "codice delle comunicazioni elettroniche"), che, all'articolo 16-*bis,* prevede l'obbligo per le imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico di adottare misure di natura tecnica e organizzativa volte a garantire la sicurezza delle reti e dei servizi di

comunicazione elettronica accessibili al pubblico, nonché di comunicare al Ministero dello sviluppo economico ogni significativa violazione della sicurezza o perdita dell'integrità delle reti. In attuazione del citato articolo 16-*bis* e dell'articolo 16-*ter* del codice delle comunicazioni elettroniche è stato adottato il decreto del Ministro dello sviluppo economico 12 dicembre 2018, che ha individuato adeguate misure di natura tecnico-organizzativa per la sicurezza e l'integrità delle reti e dei servizi di comunicazione elettronica, al fine di conseguire un livello di sicurezza delle reti adeguato al rischio esistente, e ha definito i casi in cui le violazioni della rete o la perdita dell'integrità sono da considerarsi significative ai fini della notifica al CSIRT italiano e ad altre competenti Autorità;

- il decreto legislativo 18 maggio 2018, n. 65 - di seguito "decreto legislativo NIS", di recepimento della direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. direttiva "NIS"), che, nell'individuare le misure volte a conseguire un livello elevato di sicurezza delle reti e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea, agli articoli 12 e 14 prevede obblighi di adozione di misure tecniche e organizzative in capo agli operatori di servizi essenziali e ai fornitori di servizi digitali per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza delle reti e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali e dei servizi digitali, nonché obblighi di notifica degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti. Il citato decreto legislativo, inoltre, all'articolo 8, istituisce presso la Presidenza del Consiglio dei ministri, ed in particolare presso il DIS, il CSIRT italiano, a cui è attribuito il compito di svolgere le funzioni del *computer emergency response team* (CERT) nazionale, di cui all'articolo 16-*bis* del codice delle comunicazioni elettroniche e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del decreto legislativo n. 82 del 2005, nonché le funzioni di cui all'allegato I, punto 2, del decreto legislativo n. 65 del 2018;
- il decreto del Presidente del Consiglio dei ministri 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" all'articolo 3, comma 1, lettera *b*), ha previsto che il Presidente del Consiglio dei ministri, su proposta del Comitato interministeriale per la sicurezza della Repubblica, adotti il Quadro strategico nazionale per la sicurezza dello spazio cibernetico (la cui adozione è stata successivamente prevista, a livello primario, dal decreto legislativo NIS, all'articolo 6 del decreto legislativo n. 65 del 2018), nell'ambito del quale è stato richiesto il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema Paese. In attuazione dell'articolo 3, comma 1, lettera *c*), da ultimo con decreto del Presidente del Consiglio dei ministri 31 marzo 2017, è stato adottato il Piano nazionale per la protezione cibernetica e la sicurezza informatica. In attuazione dell'articolo 11, comma 2, del citato DPCM 17 febbraio 2017, con decreto del Ministro dello sviluppo economico del 15 febbraio 2019, è stato istituito, presso l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione, il Centro di valutazione e certificazione nazionale (CVCN), che, in ambito perimetro, è chiamato a svolgere le sue funzioni istituzionali di

verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici inclusi nell'elenco dei beni ICT, al fine di rendere il relativo approvvigionamento più sicuro;

- il decreto del Presidente del Consiglio dei ministri 26 settembre 2019, con cui sono state delegate al Ministro per l'innovazione tecnologica e la digitalizzazione le funzioni spettanti al Presidente del Consiglio dei ministri in materia di innovazione digitale, all'articolo 1, comma 3, lettera *c*), ha, in particolare, delegato al predetto Ministro le funzioni e i compiti demandati alla Presidenza del Consiglio dei ministri ai fini della attuazione del decreto-legge;
- da ultimo, il regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, in attuazione dell'articolo 1, comma 2, del decreto-legge, pubblicato nella *Gazzetta Ufficiale* n. 261, del 21 ottobre 2020. Con tale provvedimento sono state definite le modalità e i criteri procedurali di individuazione dei soggetti da includere nel perimetro di sicurezza nazionale cibernetica e sono stati individuati i criteri con i quali tali soggetti predispongono e aggiornano l'elenco dei beni ICT;

3) Incidenza delle norme proposte sulle leggi e i regolamenti vigenti.

Il presente decreto, come anticipato, si muove lungo le direttrici dispositive tracciate dal decreto-legge, attuando le previsioni ivi contenute.
A tal riguardo, il decreto-legge, all'articolo 1, comma 8, ha introdotto delle disposizioni volte a coordinare gli obblighi che discendono dall'inclusione dei soggetti nel perimetro di sicurezza nazionale cibernetica con quelli derivanti in capo ai medesimi soggetti:
- dal decreto legislativo NIS, circa l'obbligo di notificare gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti e di adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi;
- dal codice delle comunicazioni elettroniche e delle correlate disposizioni attuative, relativi all'obbligo di comunicare ogni significativa violazione della sicurezza o perdita dell'integrità delle reti e dei servizi di comunicazione elettronica accessibili al pubblico e di adottare adeguate misure di natura tecnica e organizzativa per assicurare la sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico, nonché per garantire l'integrità delle stesse reti.
Nello specifico, il decreto-legge ha previsto che l'assolvimento dell'obbligo di notifica ai sensi dell'articolo 1, comma 3, lettera *a*), del decreto-legge degli obblighi di notifica previsti dal decreto legislativo NIS e dal codice delle comunicazioni elettroniche. Conseguentemente, lo schema di decreto ha provveduto a specificare che, qualora l'incidente rilevi anche ai fini del decreto legislativo NIS, ovvero del codice delle comunicazioni elettroniche, nell'effettuare la notifica al CSIRT italiano, indicano rispettivamente l'autorità competente NIS (alla quale il CSIRT italiano provvederà ad inoltrare la notifica). In via meramente ricognitiva, viene, inoltre, precisato che restano fermi gli obblighi di notifica, secondo le relative procedure, previsti dal decreto legislativo NIS e dal codice delle comunicazioni elettroniche e relative disposizioni

attuative per quegli incidenti che non rientrano nell'ambito di applicazione del decreto-legge.

Con riferimento alle misure di sicurezza, il decreto-legge ha stabilito che i soggetti inclusi nel perimetro osservano le misure di sicurezza previste dal decreto legislativo NIS e dal codice delle comunicazioni elettroniche, ove di livello almeno equivalente a quelle adottate ai sensi dell'articolo 1, comma 3, lettera *b*), del decreto-legge, facendo salva, tuttavia, la possibilità da parte della Presidenza del Consiglio dei ministri, per i soggetti pubblici e per quelli di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, e del Ministero dello sviluppo economico, per i soggetti privati, di individuare eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal decreto-legge.

4) Analisi della compatibilità dell'intervento con i principi costituzionali

Il provvedimento è stato predisposto nel rispetto dei principi costituzionali.

5) Analisi delle compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.

Il decreto non presenta aspetti di interferenza o di incompatibilità con le competenze costituzionali delle Regioni poiché incide sulla materia "sicurezza dello Stato", riservata alla competenza legislativa esclusiva dello Stato ai sensi dell'art. 117, comma 2, lettera *d*), della Costituzione. In virtù del parallelismo tra competenza legislativa esclusiva e potestà regolamentare, sancita dall'art. 117, comma 6, della Costituzione, la potestà regolamentare in materia di perimetro di sicurezza nazionale cibernetica spetta allo Stato.

6) Verifica della compatibilità con i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.

Non si ravvisano elementi di incompatibilità.

7) Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.

Trattandosi di intervento normativo di tipo attuativo, vertente peraltro su una tematica (perimetro di sicurezza nazionale cibernetica) sulla quale antecedentemente all'entrata in vigore del decreto-legge non si è legiferato, si esclude che il presente decreto possa costituire una rilegificazione, ovvero che possa qualificarsi quale intervento di delegificazione.

8) Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.

Non vi sono elementi da segnalare.

9) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo oggetto.

Non vi sono elementi da segnalare.

PARTE II - CONTESTO NORMATIVO COMUNITARIO E INTERNAZIONALE

1) Analisi della compatibilità dell'intervento con l'ordinamento comunitario

Non si ravvisano elementi di incompatibilità, poiché, ai sensi dell'articolo 4, paragrafo 2, del Trattato sull'Unione europea, la materia della "sicurezza nazionale" resta di esclusiva competenza di ciascuno Stato membro.
Con l'intervento in esame viene data attuazione ad una disciplina – quella contenuta nel decreto-legge – che appare complementare rispetto al quadro ordinamentale introdotto con la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione – recepita nell'ordinamento interno con il decreto legislativo 18 maggio 2018, n. 65 – poiché vengono stabiliti, per finalità di sicurezza nazionale, gli adempimenti attuativi necessari a garantire i nuovi e più elevati livelli di tutela e di sicurezza delle reti, sistemi informativi e servizi informatici introdotti dal decreto-legge. Analoghe considerazioni valgono anche per quanto riguarda la compatibilità del presente decreto con il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (c.d. "Cybersecurity Act").

2) Verifica dell'esistenza di procedure di infrazione da parte della Commissione europea sul medesimo o analogo oggetto.

Non risultano procedure di infrazione da parte della Commissione europea sul medesimo o analogo oggetto.

3) Analisi della compatibilità dell'intervento con gli obblighi internazionali.

Il provvedimento non presenta profili di incompatibilità con gli obblighi internazionali.

4) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia dell'Unione europea sul medesimo o analogo oggetto.

Non risultano pendenti giudizi innanzi alla Corte di Giustizia dell'Unione europea sul medesimo o analogo oggetto.

5) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte europea dei diritti dell'uomo sul medesimo o analogo oggetto.

Non vi sono elementi da segnalare.

6) Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione europea.

Non vi sono elementi da segnalare.

PARTE III - ELEMENTI DI QUALITÀ SISTEMATICA E REDAZIONALE DEL TESTO

1) Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.

L'articolo 1 dello schema di decreto mutua la maggior parte delle definizioni, per esigenze di coerenza, dal regolamento adottato con il DPCM n. 131 del 2020, in attuazione dell'articolo 1, comma 2, del decreto-legge, e al contempo riformula alcune delle definizioni ivi recate al fine di tenere conto dell'avvenuta adozione del richiamato regolamento, e introduce altre mirate definizioni ritenute rilevanti ai fini della elaborazione dei contenuti del presente decreto.

Nello specifico, rispetto al citato regolamento, è stata adeguata la definizione di "*bene ICT*", già recata dal DPCM n. 131 del 2020, al fine di tenere conto dell'inserimento, da parte di ciascuno dei soggetti inclusi nel perimetro, dei beni ICT nell'elenco di cui all'articolo 1, comma 2, lettera *b*), del decreto-legge. Sono state introdotte, poi, le definizioni di "*soggetti inclusi nel perimetro*", al fine di dare conto dell'avvenuta inclusione dei soggetti di cui all'articolo 1, comma 2, lettera *a*), del decreto-legge, nell'atto amministrativo di cui all'articolo 1, comma 2-*bis*, del medesimo decreto-legge, e di "*impatto sul bene ICT*", al fine di individuare l'ambito di operatività della disposizione di cui all'articolo 1, comma 3, lett. *a*), del decreto-legge che impone l'obbligo di notifica al CSIRT italiano degli incidenti "*aventi impatto sui beni ICT*".

2) Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni ed integrazioni subite dai medesimi.

Lo schema di decreto del Presidente del Consiglio dei ministri fa corretto riferimento alla legislazione nazionale vigente.

3) Ricorso alla tecnica della novella legislativa per introdurre modificazioni ed integrazioni a disposizioni vigenti.

Non vi sono elementi da segnalare.

4) Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.

Non vi sono elementi da segnalare.

5) Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.

Non vi sono elementi da segnalare.

6) Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo.

Non vi sono elementi da segnalare.

7) Indicazione degli eventuali atti successivi attuativi, verifica della congruenza dei termini previsti per la loro adozione.

Il presente decreto non prevede successivi atti attuativi. La tassonomia degli incidenti di cui all'articolo 2, le misure di sicurezza da applicare per ciascun bene ICT di cui all'articolo 7 e le misure di sicurezza minime per la tutela delle informazioni di cui all'articolo 9 sono puntualmente indicate, rispettivamente, negli allegati A, B e C del presente decreto.

8) Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche con correlata indicazione nella relazione economico-finanziaria della sostenibilità dei relativi costi.

Per la predisposizione dell'intervento normativo sono stati considerati i dati in possesso delle Amministrazioni coinvolte nell'attuazione delle disposizioni del decreto-legge.

Presidenza del Consiglio dei Ministri

DIPARTIMENTO PER GLI AFFARI GIURIDICI E LEGISLATIVI

IL CAPO DEL DIPARTIMENTO

Visto l'articolo 6, comma 1, lettera c), del decreto del Presidente del Consiglio dei ministri 15 settembre 2017, n. 169, che dispone l'esclusione dell'AIR per i provvedimenti normativi concernenti "disposizioni direttamente incidenti su interessi fondamentali in materia di sicurezza interna ed esterna dello Stato";

Considerato che 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 medesimo decreto-legge 21 settembre 2019, n. 105, concerne disposizioni necessarie per la sicurezza interna dello Stato;

DICHIARA

l'esclusione dall'AIR per 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 medesimo decreto-legge 21 settembre 2019, n. 105.

Roma,

Pres. Ermanno de Francisco