RELAZIONE ILLUSTRATIVA

Il decreto del Presidente del Consiglio dei ministri viene adottato ai sensi dell'articolo 1, comma 2, 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" (di seguito decreto-legge).

Il decreto-legge istituisce (articolo 1, comma 1) un "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 l'interesse dello Stato, e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Lo schema di decreto è rivolto a dare attuazione a due previsioni del decreto-legge:

- ai sensi dell'articolo 1, comma 2, lettera *a*), definisce modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica che, per questo, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge;
- ai sensi dell'articolo 1, comma 2, lettera *b*), definisce i criteri con i quali i soggetti, una volta individuati ai fini dell'inclusione nel perimetro, predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, rilevanti per le finalità della normativa introdotta dal decreto-legge e in relazione ai quali opereranno le misure e gli obblighi da essa previsti.

L'attuazione della normativa sul perimetro di sicurezza nazionale cibernetica è demandata, con scadenze temporali diversificate, a quattro decreti del Presidente del Consiglio dei ministri – di cui il presente costituisce quello a scadenza più ravvicinata – e ad un regolamento, da emanarsi ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400.

Il decreto in discorso viene adottato, come previsto dal citato decreto-legge, nella forma del decreto del Presidente del Consiglio dei ministri, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR). Per la parte riguardante la definizione dei criteri per la predisposizione e l'aggiornamento degli elenchi dei beni ICT rilevanti, di cui all'articolo 1, comma 2, lettera *b*), del decreto-legge, inoltre, la proposta di decreto prevede, in fase istruttoria, che all'elaborazione di tali criteri provveda l'organismo tecnico di supporto al Comitato interministeriale, adottando gli opportuni moduli organizzativi, integrato con un rappresentante della Presidenza del Consiglio dei ministri: si tratta di un rappresentante della struttura della Presidenza del Consiglio competente per la in-

novazione tecnologica e la digitalizzazione, designato in ragione degli specifici compiti attribuiti alla Presidenza del Consiglio dal decreto-legge.

Il richiamato riferimento legislativo è all'organismo (c.d. CISR tecnico) istituito presso il Dipartimento delle informazioni per la sicurezza (DIS) di cui all'articolo 4 della legge 3 agosto 2007, n. 124, con compiti di supporto al Comitato interministeriale ai sensi dell'articolo 4, comma 5, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 26 ottobre 2012, n. 2, recante l'ordinamento e l'organizzazione del DIS (citata disposizione in all. 1). L'organismo è ora previsto dall'articolo 4, comma 5, del regolamento adottato con DPCM 3 aprile 2020, n. 2, che definisce l'ordinamento e l'organizzazione del DIS, (citata disposizione in all. 2) adottato ai sensi dell'articolo 43 della citata legge n. 124/2007, della cui emanazione è stata data comunicazione nella Gazzetta Ufficiale del 10 aprile scorso.

Sullo schema del decreto deve intervenire, secondo la previsione di cui al comma 4-*bis* dell'articolo 1, aggiunta nei lavori parlamentari di conversione del decreto-legge, il parere delle Commissioni parlamentari competenti della Camera e del Senato. La medesima disposizione, modificata nei lavori parlamentari di conversione del decreto-legge 30 dicembre 2019, n. 162 (c.d. decreto milleproroghe 2020), prevede, infine, che lo schema di decreto venga anche trasmesso al Comitato parlamentare per la sicurezza della Repubblica.

La proposta di decreto, in particolare dopo l'intervento emendativo apportato con il citato decreto-legge n. 162 – che, per ciò che riguarda l'individuazione dei soggetti inclusi nel perimetro, ha separato in due distinti atti, da un lato, la definizione delle modalità e dei criteri procedurali e, dall'altro, la concreta individuazione degli stessi soggetti – appare presentare indici che inducono a ritenerne il possibile carattere normativo.

A questo riguardo, la disciplina definita dal decreto-legge è improntata ad un carattere di progressiva attuazione: sia l'individuazione dei soggetti inclusi nel perimetro che la predisposizione degli elementi dei beni ICT, che saranno soggetti alla disciplina prevista dal decreto-legge, avvengono sulla base di un criterio di gradualità; gli elenchi dei beni ICT vengono aggiornati con cadenza almeno annuale. Infine, le stesse modalità e i criteri procedurali, ed i criteri di cui al decreto in discorso sono oggetto di aggiornamento, con le medesime modalità di adozione del decreto originario, con cadenza almeno biennale[1].

In tale contesto, è stato comunque considerato che il decreto appare rivolto a disciplinare innovativamente, e con carattere di generalità, quanto ai soggetti cui si indirizza, e di ripetibilità in un numero indefinito di casi – si intende nel periodo di vigenza dello stesso decreto e fino all'aggiornamento – sia l'inclusione nel perimetro di sicurezza nazionale cibernetica delle amministrazioni pubbliche, degli enti e degli operatori pubblici e priva-

---

[1] Per completezza, analoga previsione di periodico aggiornamento è contemplata riguardo al DPCM di cui all'articolo 1, comma 3, in materia di definizione delle procedure di notifica degli incidenti e delle misure di sicurezza.

ti, dettando a tal fine le relative modalità e i criteri procedurali, sia l'individuazione, da parte di questi ultimi, delle reti, dei sistemi informativi e dei servizi informatici, ai cui fini il decreto fissa i relativi criteri.

Sotto il profilo sistematico lo schema di decreto, che si compone complessivamente di 12 articoli, è suddiviso in quattro Capi, di cui il Capo II e il Capo III dedicati, rispettivamente, alla definizione delle "Modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica", ed alla definizione dei "Criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e di servizi informatici". Il Capo I e il Capo IV sono invece dedicati, rispettivamente, all'individuazione delle "Definizioni e criteri generali" ed alla definizione delle "Disposizioni sulla tutela delle informazioni, transitorie e finali".

L'articolo 1 contiene le definizioni utili impiegate nel testo. Si richiamano, al riguardo, le più rilevanti ai fini della elaborazione dei contenuti del decreto e, in particolare quelle di:

- "pregiudizio per la sicurezza nazionale", concetto cardine della disciplina del perimetro di sicurezza nazionale cibernetica (cfr. articolo 1, comma 1, del decreto-legge), nonché, nello specifico, parametro indicato dal legislatore – "l'entità del pregiudizio per la sicurezza nazionale" che può derivare da eventi a carico dei beni ICT preordinati all'esercizio di funzioni essenziali o di servizi essenziali – per l'individuazione dei soggetti inclusi nel perimetro (articolo 1, comma 2, lettera *a*), numero 2-*bis*, del decreto-legge);
- "incidente", quale evento, di natura accidentale o intenzionale, che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici. Tali eventi sono quelli che la normativa sul perimetro si propone di fronteggiare, o di mitigarne le conseguenze sulla sicurezza nazionale, attraverso le misure, gli obblighi e le procedure previste dal decreto-legge;
- "rete e sistema informativo", mutuata dal decreto legislativo 18 maggio 2018, n. 65, di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (specificando interpretativamente, per le finalità della normativa in discorso, l'inclusione dei sistemi di controllo industriale);
- "servizio informatico", che ha recepito la definizione contenuta nel regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione – c.d. *cybersecurity act* – specificando interpretativamente, per le finalità della normativa in discorso, l'inclusione dei servizi di *cloud computing*;
- "bene ICT", che considera unitariamente, dal punto di vista della sua funzionalizzazione ai fini dello svolgimento di funzioni essenziali dello Stato o per la erogazione

di servizi essenziali, un insieme di reti, sistemi informativi e servizi informatici, o parti di essi;

- "parte minimale di un bene ICT", che identifica, secondo il meccanismo che viene descritto all'articolo 7, la più piccola porzione di una rete, di un sistema informativo o di un servizio informatico imprescindibile ai fini dell'espletamento di una funzione essenziale dello Stato o dell'erogazione di un servizio essenziale;
- "analisi del rischio", presupposto per l'individuazione, da parte dei soggetti del perimetro – secondo un criterio di gradualità, in base al meccanismo che viene descritto all'articolo 7 – delle reti, dei sistemi informativi e dei servizi informatici, in relazione ai quali gli stessi soggetti dovranno osservare le norme sul perimetro.

Gli articoli 2, 3 e 4 delineano nello specifico le modalità e i criteri procedurali per l'individuazione dei soggetti inclusi nel perimetro.

Il decreto-legge indica, all'articolo 1, comma 2, lettera *a*), nn. 1), 2), e 2-*bis*), i criteri per l'individuazione dei soggetti:

- il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;
- l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici;
- l'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alla specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti.

Al fine di dare attuazione a tale previsione, l'articolo 2, lettera a), dello schema di decreto fornisce preliminarmente un criterio interpretativo generale prevedendo che, ai fini dello stesso decreto, un soggetto esercita una funzione essenziale laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario, e dei trasporti.

Lo stesso articolo 2, lettera b), stabilisce altresì che un soggetto eroga un servizio essenziale laddove ponga in essere: attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

L'articolo 3, poi, al fine di consentire l'individuazione dei soggetti sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale, in

relazione alla specificità dei diversi settori di attività, provvede ad individuare innanzitutto i settori di attività in cui in via prioritaria – fatta salva l'estensione ad altri settori in sede di aggiornamento, previsto ai sensi dell'articolo 1, comma 5, del decreto-legge – saranno individuati, come indicato dal presente decreto, i soggetti ai fini dell'inclusione nel perimetro.

Tali settori sono individuati, al comma 1, in:

- settore governativo. Il settore comprende, in via descrittiva, le attività dell'amministrazione dello Stato, come definita dall'articolo 8, comma 1, della legge 7 agosto 2015, n. 124, includente la Presidenza del Consiglio dei ministri, i Ministeri, le agenzie governative nazionali e gli enti pubblici non economici nazionali. In applicazione del più volte richiamato criterio di gradualità, nella fase della prima individuazione dei soggetti inclusi nel perimetro, vengono prese in considerazione le attività delle amministrazioni rappresentate nel Comitato interministeriale per la sicurezza della Repubblica, avendo a parametro la composizione di tale Organo, in quanto appartenente al Sistema di informazione per la sicurezza della Repubblica, di cui all'articolo 2 della legge n. 124 /2007. Ulteriori ampliamenti dell'estensione del settore governativo potranno essere compiuti nei successivi aggiornamenti del DPCM;
- i settori *b*) difesa; *c*) spazio e aerospazio; *d*) energia; *e*) telecomunicazioni; *f*) economia e finanza; *g*) trasporti; *h*) servizi digitali; *i*) tecnologie critiche; *l*) enti previdenziali/lavoro.

L'articolo 3, comma 2, attribuisce poi la competenza ad individuare, secondo le modalità e i criteri procedurali indicati all'articolo 4, i soggetti inclusi nel perimetro, operanti in ciascun settore ai seguenti Ministeri:

a) per il settore governativo, le amministrazioni rappresentate nel CISR, ciascuna nell'ambito di rispettiva competenza;

b) per il settore difesa, il Ministero della difesa;

c) per il settore spazio e aerospazio, la Presidenza del Consiglio dei ministri, ai sensi della legge 11 gennaio 2018, n. 7;

d) per il settore energia, il Ministero dello sviluppo economico;

e) per il settore telecomunicazioni, il Ministero dello sviluppo economico;

f) per il settore economia e finanza, il Ministero dell'economia e delle finanze;

g) per il settore trasporti, il Ministero delle infrastrutture e dei trasporti;

h) per il settore servizi digitali, il Ministero dello sviluppo economico, in raccordo con la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione;

i) per il settore tecnologie critiche, la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, in raccordo con il Ministero dello sviluppo economico e con il Ministero dell'università e della ricerca;

l) per il settore enti previdenziali/lavoro, il Ministero del lavoro.

In particolare, per quanto riguarda il settore governativo, ciascuna delle amministrazioni CISR individuerà, nell'ambito delle proprie attività o riconducibili alla propria sfera di competenza nell'ambito governativo (cioè dell'Amministrazione dello Stato), le amministrazioni o gli enti che esercitano funzioni essenziali dello Stato di cui all'articolo 2, comma 1, lettera *a*), ovvero che svolgono servizi essenziali come definiti all'articolo 2, comma 1, lettera *b*).

Per tutti gli altri settori, il Ministero competente, anche in raccordo, ove individuati, con gli altri Ministeri indicati, individuerà gli altri soggetti, pubblici o privati, che svolgono le attività di cui all'articolo 2, comma 1, nell'ambito di ciascun settore. Esemplificando, il Ministero della difesa individuerà, per quanto di propria competenza, nell'ambito delle attività governative di cui all'articolo 3, comma 1, le strutture e gli enti che fanno capo all'amministrazione militare, mentre nell'ambito del settore difesa di cui all'articolo 3, comma 2, lettera *b*), individuerà i soggetti, pubblici o privati, che svolgono attività strumentali all'esercizio di funzioni essenziali dello Stato (in questo caso della difesa dello Stato); sempre esemplificativamente, il Ministero dello sviluppo economico individuerà, nell'ambito del settore governativo, eventuali proprie strutture che esercitano funzioni essenziali e, nel settore energia, i soggetti pubblici o privati che esercitano servizi essenziali o in quanto strumentali all'esercizio di funzioni essenziali dello Stato, ovvero consistenti in attività necessarie per il mantenimento di attività economiche fondamentali o per la continuità degli approvvigionamenti etc.

L'articolo 4 declina le modalità ed i criteri procedurali che consentiranno alle amministrazioni – cui è attribuita la competenza in base all'articolo 3, comma 2 – l'individuazione dei soggetti, prevedendo in merito una clausola di salvaguardia della specifica disciplina relativa agli Organismi di informazione e sicurezza di cui alla legge n. 124/2007, la cui applicazione è espressamente contemplata dall'art. 1, comma 2, lettera *a*), del decreto-legge.

In applicazione dei criteri legislativamente previsti viene definito un modello che, nei settori di attività di rispettiva competenza, ai sensi del citato art. 3, comma 2, del DPCM, le amministrazioni saranno tenute ad osservare per pervenire all'individuazione dei soggetti secondo un criterio di gradualità. In base all'articolo 4, comma 1, lettera *a*), il modello si fonda sulla identificazione, da parte delle amministrazioni, delle funzioni essenziali e dei servizi essenziali di diretta pertinenza, ovvero esercitate o prestati da soggetti vigilati o da operatori anche privati – che dipendono da reti, sistemi informativi o servizi informatici – la cui interruzione o compromissione possa arrecare un pregiudizio per la sicurezza nazionale.

Detto pregiudizio verrà valutato dalle amministrazioni attraverso l'applicazione dei criteri di seguito indicati, tenendo conto della rilevanza di ciascun criterio in relazione agli specifici settori di attività. In merito, si prevede (articolo 4, comma 1, lettera *b*), numero 1), che vengano presi in considerazione gli effetti di una interruzione della funzione essenziale o del servizio essenziale, valutando in proposito elementi quali l'estensione territoriale della funzione essenziale o del servizio essenziale, il numero e la tipologia di utenti potenzialmente interessati, i livelli di servizio garantiti ove previsti, le possibili ricadute economiche, ove applicabili, nonché ogni altro elemento rilevante, in relazione a ciascun settore, ai fini della valutazione di un possibile danno o pericolo di

danno ai beni ed interessi di cui all'articolo 1, comma 1, lettera *f*) (indipendenza, integrità o sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero interessi politici, militari, economici, scientifici e industriali dell'Italia). Si prevede poi (articolo 4, comma 1, lettera *b*), numero 2), che vengano presi in considerazione anche gli effetti della compromissione dello svolgimento della funzione essenziale o del servizio essenziale, valutando le conseguenze della perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni trattate per il loro svolgimento, avuto riguardo alla tipologia ed alla quantità degli stessi, alla loro sensibilità ed allo scopo cui sono destinati.

Per altro verso, le amministrazioni valuteranno la possibile mitigazione (articolo 4, comma 1, lettera *b*), numero 3), rispetto all'interruzione o alla compromissione dello svolgimento della funzione essenziale o del servizio essenziale. Tale valutazione, in particolare, sarà effettuata avuto riguardo al tempo necessario per ripristinarne lo svolgimento in condizioni di sicurezza, alla possibilità che lo svolgimento della funzione essenziale o del servizio essenziale possano o meno essere assicurati, anche temporaneamente, con modalità prive di supporto informatizzato, ovvero, anche parzialmente, da altri soggetti.

Alla luce di quanto sopra, le amministrazioni individueranno (articolo 4, comma 1, lettera *c*) le funzioni essenziali e i servizi essenziali per i quali, in caso di interruzione o compromissione, il pregiudizio per la sicurezza nazionale sarà ritenuto massimo e le possibilità di mitigazione minime. Gli stessi funzioni e servizi verranno quindi graduati in una scala crescente e saranno individuati (articolo 4, comma 1, lettera *d*), i soggetti che li svolgono.

Secondo il canone della gradualità, in fase di prima applicazione è, infine, previsto che siano individuati, ai fini dell'inclusione nel perimetro, soltanto i soggetti titolari delle funzioni essenziali o dei servizi essenziali, un'interruzione delle cui attività comporterebbe il mancato svolgimento della funzione o del servizio.

L'articolo 5 disciplina la fase di predisposizione dell'elenco dei soggetti del perimetro di cui all'articolo 1, comma 2-*bis*, del decreto-legge. L'elencazione dei soggetti è contenuta in un decreto del Presidente del Consiglio dei ministri, di natura non regolamentare, adottato – entro trenta giorni dalla data di entrata in vigore del presente decreto – ed aggiornato su proposta del CISR.

Sul punto, l'articolo 5 prevede che, le amministrazioni di cui all'articolo 3, comma 2, in relazione ai settori di attività di competenza, predispongono, per la sottoposizione al CISR ai fini della formulazione della citata proposta al Presidente del Consiglio dei ministri, una lista di soggetti individuabili ai sensi dell'articolo 4, e la trasmettono al CISR tecnico.

La comunicazione di avvenuta iscrizione nell'elenco dei soggetti inclusi nel perimetro è effettuata dal DIS che ne informa le amministrazioni di cui all'articolo 3, comma 2. Dell'avvenuta iscrizione è data altresì comunicazione da parte del DIS alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, per i soggetti pubblici e per quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82 (c.d. codice dell'amministrazione digitale), e

al Ministero dello sviluppo economico, per quelli privati. L'elencazione dei soggetti inclusi nel perimetro è altresì comunicata dal DIS 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.

L'articolo 6 reca l'istituzione, a supporto del CISR tecnico, del Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica, presieduto da un vice direttore generale del DIS e composto da due rappresentanti di ciascuna amministrazione CISR, da un rappresentante per ciascuna delle due Agenzie (Agenzia informazioni e sicurezza esterna e Agenzia informazioni e sicurezza interna), nonché da due rappresentanti degli altri ministeri di volta in volta interessati, che sono chiamati a partecipare alle riunioni, anche su loro richiesta motivata, in relazione agli argomenti da trattare. L'istituzione del Tavolo interministeriale corrisponde all'esigenza di disporre di un Organo composto dai rappresentanti delle amministrazioni, che siano in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, di cui lo stesso CISR tecnico – composto invece dai dirigenti apicali designati dai Ministri membri del Comitato, nonché dai Direttori delle citate Agenzie – possa avvalersi nella istruttoria in discorso e, più in generale, nella fase di attuazione di una normativa complessa e di progressiva applicazione quale quella del perimetro di sicurezza nazionale cibernetica.

Ai sensi dell'articolo 6, comma 3, il CISR tecnico si avvale del Tavolo interministeriale per l'esercizio delle funzioni istruttorie di cui all'articolo 5 – in materia di predisposizione dell'elenco dei soggetti inclusi nel perimetro, da sottoporre al CISR per la formulazione della proposta al Presidente del Consiglio – e ai fini del supporto per ogni altra attività attribuita dal decreto-legge al CISR o al CISR tecnico.

Viene previsto che il Tavolo interministeriale si riunisce periodicamente, almeno una volta ogni 6 mesi, e può essere convocato d'iniziativa del presidente o su richiesta di almeno un componente designato, in relazione alla trattazione di specifici argomenti. Alle riunioni del Tavolo interministeriale possono essere chiamati a partecipare rappresentanti di altre amministrazioni pubbliche, nonché di enti e operatori pubblici e privati.

Infine, è previsto che la partecipazione alle riunioni del Tavolo interministeriale costituisce dovere d'ufficio e non sono, pertanto, dovuti gettoni di presenza, compensi, rimborsi spese o altri emolumenti comunque denominati.

L'articolo 7 definisce i criteri per la predisposizione e l'aggiornamento, da parte dei soggetti inclusi nel perimetro, degli elenchi di beni ICT di rispettiva pertinenza di cui all'articolo 1, comma 2, lettera *b*). Il DPCM utilizza il concetto di "bene ICT", di cui è data la definizione al richiamato articolo 1, comma 1, lettera *m*), così da poter considerare, ai fini dell'inclusione nell'elenco, l'insieme di reti, sistemi informativi e servizi informatici, o di parti di essi, destinati unitariamente, dal punto di vista funzionale, a servizio dello svolgimento di una funzione essenziale o della erogazione di un servizio essenziale.

La disposizione fissa il processo con cui i predetti soggetti, a valle dell'individuazione di ciascuna funzione essenziale o servizio essenziale in relazione a cui sono inclusi nel perimetro, perverranno all'individuazione dei beni ICT da includere negli elenchi. Sono in questa sede dettati i criteri dell'analisi del rischio che ciascun soggetto effettuerà nello specifico, in relazione ai beni di pertinenza. Al riguardo, giova evidenziare che l'individuazione di tali criteri deriva da una analisi generale del rischio, ai fini dell'applicazione della normativa in discorso, che tenuto conto anche del criterio della gradualità, ha evidenziato, per una corretta valutazione, i criteri direttivi indicati all'articolo 7, comma 2.

Alla luce di quanto sopra, ricevuta la comunicazione di avvenuta iscrizione nell'elenco, i soggetti inclusi nel perimetro individueranno i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale, un evento a carico dei quali, tra gli eventi indicati dall'articolo 1, comma 1, possa comportare l'interruzione e/o la compromissione di detta funzione o servizio.

In particolare, il comma 2 specifica che i predetti soggetti valuteranno l'impatto di un incidente sul bene ICT, in termini sia di limitazione della operatività del bene, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio; le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione (articolo 7, comma 2, lettera *a*)).

L'articolo 7, comma 2, lettera *b*), primo periodo, prevede, poi, che i soggetti, nella predisposizione degli elenchi di beni ICT, individuino, ove possibile, le parti minimali di ciascun bene ICT, come definite dall'articolo 1, comma 1, lettera *n*). I soggetti inclusi nel perimetro potranno, già nella prima predisposizione dell'elenco, ove siano in grado, o comunque in sede di aggiornamento dello stesso elenco, individuare in maniera mirata esclusivamente le porzioni dei beni la cui compromissione comporti la compromissione del bene ICT, risolvendosi in un pregiudizio per lo svolgimento di una funzione essenziale o di un servizio essenziale.

Tale meccanismo consentirà ai soggetti di corrispondere pienamente a quanto previsto dal decreto-legge, minimizzando al contempo le reti, i sistemi e i servizi informatici che in concreto saranno assoggettati, per le finalità di sicurezza nazionale, ai conseguenti obblighi previsti dalla normativa del perimetro di sicurezza nazionale cibernetica.

Sempre in linea con il criterio di gradualità, è previsto che, in fase di prima applicazione, siano individuati i beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale, o una compromissione degli stessi con effetti irreversibili sotto il profilo della integrità o della riservatezza dei dati e delle informazioni.

L'articolo 7, infine, richiama la clausola di salvaguardia prevista dall'articolo 1, comma 2, lettera *b*), del decreto-legge, ai sensi del quale è stabilito che per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, continui ad applicarsi quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l*), della legge n. 124/2007.

Gli articoli 8 e 9 definiscono i contenuti e le modalità di trasmissione degli elenchi di cui al richiamato articolo 1, comma 2, lettera *b*), del decreto-legge.

L'articolo 8, comma 1, prevede che l'architettura e la componentistica relative ai beni ICT siano descritte conformemente al modello predisposto e periodicamente aggiornato dal DIS, sentito il CISR tecnico, che ne cura anche la comunicazione ai soggetti interessati. Ai sensi dell'articolo 8, comma 2, il predetto modello individua altresì le informazioni necessarie ai fini della trasmissione degli elenchi prevista dall'articolo 9.

Per ragioni di riservatezza e razionalizzazione, la trasmissione viene effettuata tramite una piattaforma digitale costituita presso il DIS anche per le attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica. Tali modalità di trasmissione si applicano anche per l'aggiornamento degli elenchi di beni ICT e del modello di cui all'articolo 8, comma 2.

L'articolo 9, comma 2, prevede che la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione e il Ministero dello sviluppo economico accedono alla piattaforma digitale, per i profili di competenza (lo svolgimento delle attività di ispezione e verifica previste dall'articolo 1, comma 6, lettera c), nonché i compiti di cui all'articolo 1, comma 12, del decreto-legge, relativi all'accertamento delle violazioni ed alla irrogazione delle sanzioni amministrative).

L'articolo 9, comma 3, stabilisce che per ciò che riguarda le reti, i sistemi informativi e i servizi informatici 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 di cui all'articolo 1, comma 6, lettera *c*), del decreto-legge – relativamente ai quali le attività di ispezione e verifica sono 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 – la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione accede alla piattaforma digitale limitatamente alle informazioni necessarie, individuate dal modello di cui all'articolo 8, comma 2, per lo svolgimento dei compiti previsti dall'articolo 1, comma 12, del decreto-legge.

L'articolo 9, comma 4, prevede, infine, che l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del D.L. n. 144/2005 accede per il tramite della piattaforma digitale agli elenchi di beni ICT e fornisce alla stessa piattaforma gli elenchi di pertinenza del Ministero.

L'articolo 10 stabilisce, in tema di tutela delle informazioni, 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 – siano sottoposti ad idonee misure di sicurezza, previste con decreto del Presidente del Consiglio dei ministri adottato ai sensi dell'articolo 1, comma 3, del decreto-legge. È fatta salva l'adozione delle misure di sicurezza previste in caso di attribuzione agli elenchi di classifiche di segretezza ai sensi dell'articolo 42 della legge n. 124/2007.

L'articolo 11 contiene disposizioni di carattere transitorio previste a fini di coordinamento. In particolare, stabilisce che i soggetti inclusi nel perimetro osservano

in relazione alle reti, ai sistemi informativi e ai servizi informatici di cui all'articolo 1, comma 2, lettera *b*), del decreto-legge, gli obblighi in materia di notifica degli incidenti, di misure di sicurezza, nonché di affidamento delle forniture previsti dall'articolo 1, commi 3 e 6 del decreto-legge, a decorrere dalle date che saranno indicate dai provvedimenti previsti dalle medesime disposizioni.

L'articolo 12, infine, indica che dal presente decreto non derivano nuovi o maggiori oneri per la finanza pubblica.

RELAZIONE TECNICA

Il decreto del Presidente del Consiglio dei ministri viene adottato ai sensi dell'articolo 1, comma 2, 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" (di seguito decreto-legge).

Il decreto-legge istituisce (articolo 1, comma 1) un "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 l'interesse dello Stato, e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Il decreto, che viene adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), è rivolto a dare attuazione a due previsioni del decreto-legge:

- ai sensi dell'articolo 1, comma 2, lettera *a*), definisce modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica che, per questo, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge;
- ai sensi dell'articolo 1, comma 2, lettera *b*), definisce i criteri con i quali i soggetti, una volta individuati ai fini dell'inclusione nel perimetro, predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, rilevanti per le finalità della normativa introdotta dal decreto-legge e in relazione ai quali opereranno le misure e gli obblighi da essa previsti.

All'adempimento degli obblighi previsti dalle disposizioni del decreto-legge n. 105/2019, come riportato nella relazione tecnica allegata allo stesso provvedimento legislativo, è previsto che i soggetti pubblici interessati provvederanno nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente, secondo gli ambiti di competenza delineati dallo stesso decreto-legge.

Anche per quanto concerne l'osservanza degli obblighi previsti dal presente decreto gli stessi soggetti pubblici provvederanno quindi nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente e, pertanto, le disposizioni del provvedimento non comportano nuovi o maggiori oneri a carico della finanza pubblica.

Anche la costituzione del Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica (art. 6 del DPCM) non comporterà nuovi oneri, atteso che è espressamente previsto (art. 6, comma 6) che la partecipazione alle riunioni del Tavolo costituisce dovere d'ufficio e non sono, pertanto, dovuti gettoni di presenza, compensi, rimborsi spese o altri emolumenti comunque denominati.

ANALISI TECNICO-NORMATIVA

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 ai sensi dell'articolo 1, comma 2, 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.

Lo schema di decreto è rivolto a dare attuazione a due previsioni del decreto-legge n. 105/2019:

- ai sensi dell'articolo 1, comma 2, lettera *a*), definisce modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica che, per questo, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge;
- ai sensi dell'articolo 1, comma 2, lettera *b*), definisce i criteri con i quali i soggetti, una volta individuati ai fini dell'inclusione nel perimetro, predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, rilevanti per le finalità della normativa introdotta dal decreto-legge e in relazione ai quali opereranno le misure e gli obblighi da essa previsti, comprensivo della relativa architettura e componentistica.

Il decreto, ai sensi dell'articolo 1, comma 5, del decreto-legge n. 105/2019, è soggetto ad aggiornamento periodico, con cadenza almeno biennale, con le medesime modalità di adozione del decreto originario. In tale contesto, il provvedimento reca una disciplina avente carattere di innovatività rispetto all'ordinamento vigente, di generalità, quanto ai soggetti destinatari, e di replicabilità in un numero indefinito di casi, nel periodo di vigenza e fino all'aggiornamento.

Trattandosi di intervento attuativo del decreto legge n. 105/2019, l'adozione del DPCM 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 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, possa derivare un pregiudizio per la sicurezza nazionale.

2) Analisi del quadro normativo nazionale.

Il decreto-legge n. 105/2019, cui il decreto in discorso dà attuazione, integra organicamente, in una prospettiva di sicurezza nazionale, il quadro normativo vigente in tema di sicurezza cibernetica prevedendo le misure necessarie per assicurare elevati livelli di sicurezza informatica di reti, sistemi informativi e servizi informatici di interesse strategico, al fine di evitare che dalla presenza di possibili vulnerabilità possano derivare pregiudizi per la sicurezza nazionale.

Vengono, a tal fine, definite adeguate misure di sicurezza, procedure per la tempestiva informazione agli organi competenti degli incidenti informatici, nonché disposizioni per un procurement più sicuro di prodotti, processi e servizi ICT destinati alle suddette infrastrutture.

Il decreto legislativo 15 settembre 2003, n. 259, 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 adeguate misure di natura tecnica e organizzativa per 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.

Il decreto legislativo 7 marzo 2005, n. 82, all'articolo 14-*bis*, assegna all'Agenzia per l'Italia Digitale il compito di promuovere l'innovazione digitale nel Paese e l'utilizzo delle tecnologie digitali nell'organizzazione della pubblica amministrazione, attribuendole inoltre, ai sensi dell'articolo 29 dello stesso decreto, il compito di qualificare e accreditare i soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata o di gestore dell'identità digitale, nonché i soggetti che intendono svolgere l'attività di conservatore di documenti informatici.

La legge 3 agosto 2007, n. 124, modificata dalla legge 7 agosto 2012, n. 133, all'articolo 4, comma 3, lettera d-*bis*), attribuisce al Dipartimento delle informazioni per la sicurezza il compito di coordinare le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

Il decreto legislativo 18 maggio 2018, n. 65, di recepimento della direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. direttiva "NIS"), agli articoli 12 e 14, prevede obblighi di adozione di misure tecniche e organizzative in capo agli operatori di servizi essenziali ed ai fornitori di servizi digitali, al fine di prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura dei servizi essenziali e dei servizi digitali e obblighi di notifica degli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti. Inoltre, all'articolo 8, istituisce il Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT italiano), cui è attribuito anche il compito di svolgere le funzioni del Computer Emergency Response Team (CERT) nazionale, di cui all'articolo 16-*bis* del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del D. Lgs. n. 82/2005.

Il DPCM 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" prevede la definizione di un Quadro strategico nazionale

per la sicurezza dello spazio cibernetico, 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. Con DPCM 27 gennaio 2014 è stato inoltre adottato il Piano nazionale per la protezione cibernetica e la sicurezza informatica, sostituito dal DPCM 31 marzo 2017, con il quale è stato indicato l'indirizzo operativo di revisionare e consolidare la legislazione esistente in materia di sicurezza informatica e di definire un quadro giuridico adeguato per supportare le attività di sicurezza in materia cyber. Lo stesso DPCM 17 febbraio 2017 attribuisce all'organismo collegiale di coordinamento (CISR-tecnico) – di cui all'articolo 4, comma 5, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 26 ottobre 2012, n. 2, recante l'ordinamento e l'organizzazione del Dipartimento delle informazioni per la sicurezza – il compito di supportare il CISR nello svolgimento delle funzioni di proposta, deliberazione e controllo nel settore della sicurezza informatica nazionale. L'organismo è ora previsto dall'articolo 4, comma 5, del regolamento adottato con DPCM 3 aprile 2020, n. 2, che definisce l'ordinamento e l'organizzazione del DIS, adottato ai sensi dell'articolo 43 della citata legge n. 124/2007, della cui emanazione è stata data comunicazione nella Gazzetta Ufficiale del 10 aprile scorso.

Il Decreto del Ministro dello sviluppo economico 12 dicembre 2018, in attuazione degli articoli 16-*bis* e 16-*ter* del D.Lgs. n. 259/2003, 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 da parte dei fornitori di reti e servizi di comunicazione alle competenti Autorità.

Il Decreto del Ministro dello sviluppo economico 15 febbraio 2019, in attuazione dell'articolo 11 del DPCM 12 febbraio 2017, ha istituito, presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione, il Centro di Valutazione e Certificazione Nazionale (CVCN) per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale.

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

Non vi sono elementi da segnalare.

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

Il provvedimento è stato predisposto nel rispetto dei principi costituzionali. **Vedasi anche quanto sub 5).**

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

Non si ravvisano elementi di incompatibilità. La disciplina in tema di perimetro di sicurezza nazionale cibernetica, attenendo alla materia "sicurezza dello Stato", è rimessa

alla potestà legislativa esclusiva dello Stato ai sensi dell'art. 117, comma 2, lettera d), della Costituzione e, nelle materie di competenza legislativa esclusiva statale, la potestà regolamentare spetta allo Stato, ai sensi dell'art. 117, comma 6, della Costituzione.

6) Verifica della compatibilità con i principi di sussidiarietà, differenziazione e 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 natura regolamentare esso non comporta rilegificazioni. Il DPCM, inoltre, non ha natura di regolamento in delegificazione. Per finalità di semplificazione normativa è stato utilizzato il ricorso ad una fonte separata (articolo 8 del DPCM) in merito alla definizione del modello per la descrizione dell'architettura e della componentistica relative ai beni ICT individuati negli elenchi di cui all'articolo 7, comma 2, lettera b), e alle modalità di trasmissione degli stessi elenchi ai sensi dell'articolo 9 del DPCM . Ciò consentirà, trattandosi di disposizioni di natura tecnica, di aggiornare il modello in relazione all'evoluzione tecnologica senza dover seguire il procedimento di adozione previsto per l'aggiornamento del DPCM.

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

Il 5 marzo 2020 risulta essere stato presentato al Senato un disegno di legge d'iniziativa parlamentare, recante "Disposizioni in materia di sicurezza nazionale volte a rafforzare la tutela degli interessi strategici economici ed il ruolo del Parlamento" (A.S. n. 1759). In merito all'iter di approvazione, agli atti parlamentari risulta che il provvedimento sia da assegnare alle competenti Commissioni parlamentari.

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 D.L. n. 105/2019 – 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, stabilendo, per finalità di sicurezza nazionale, nuovi e più elevati livelli di tutela e di sicurezza per reti, sistemi e servizi rilevanti. Analoghe considerazioni valgono anche per quanto riguarda la compatibilità del decreto-legge n. 105 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 cibersicurezza, e alla certificazione della cibersicurezza 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 vi sono elementi da segnalare.

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 vi sono elementi da segnalare.

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 DPCM introduce alcune definizioni rilevanti ai fini della elaborazione dei contenuti del decreto e, tra queste, pregiudizio per la sicurezza nazionale, incidente, rete e sistema informativo, servizio informatico, bene ICT, parte minimale di un bene ICT e analisi del rischio.

Alcune delle predette definizioni sono elaborate sulla base di nozioni già consolidate nell'ambito di altri provvedimenti normativi: la definizione di "rete e sistema informativo" è, infatti, mutuata dal decreto legislativo 18 maggio 2018, n. 65, di

attuazione della direttiva NIS; quella di "servizio informatico" recepisce la definizione contenuta nel regolamento (UE) 2019/881 (c.d. cyber security act). Le suddette definizioni sono oggetto di una precisazione al fine di chiarire, in via interpretativa, che vi sono inclusi, rispettivamente, i "sistemi di controllo industriale" e i "sistemi di cloud computing".

La definizione di "incidente" – quale evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici – costituisce lo sviluppo, anche a fini di coordinamento, della terminologia utilizzata nel decreto-legge n. 105/2019 (art. 1 comma 3).

È stata prevista la definizione di "bene ICT", al fine di poter considerare unitariamente, dal punto di vista della sua funzionalizzazione ai fini dello svolgimento di funzioni essenziali dello Stato o per la erogazione di servizi essenziali, un insieme di reti, sistemi informativi e servizi informatici, o parti di essi.

La definizione di "parte minimale di un bene ICT" è stata elaborata, con finalità di semplificazione, allo scopo di identificare, in base al meccanismo di cui all'articolo 7, la più piccola porzione di una rete, di un sistema informativo o di un servizio informatico imprescindibile ai fini dell'espletamento di una funzione essenziale dello Stato o dell'erogazione di un servizio essenziale.

È stata, infine, prevista la definizione di "analisi del rischio", di cui il DPCM detta i criteri generali, quale presupposto per l'individuazione, da parte dei soggetti del perimetro – secondo un criterio di gradualità, in base al meccanismo di cui all'articolo 7 – delle reti, dei sistemi informativi e dei servizi informatici, in relazione ai quali gli stessi soggetti dovranno osservare le norme sul perimetro.

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.

Nello schema di provvedimento non si è fatto ricorso alla tecnica della novella normativa.

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 DPCM prevede i seguenti successivi atti attuativi:

- l'adozione, del decreto del Presidente del Consiglio dei ministri, su proposta del CISR, entro trenta giorni dalla data di entrata in vigore del DPCM in discorso, contenente l'elencazione dei soggetti individuati ai sensi di quanto previsto dallo stesso DPCM (articolo 5 del DPCM, in relazione all'articolo 1, comma 2-*bis*, del decreto-legge);
- la comunicazione da parte del DIS ai sensi dell'articolo 1, comma 2-*bis*, del decreto-legge a ciascun soggetto interessato dell'avvenuta inclusione nell'elencazione dei soggetti (articolo 5, comma 3, del DPCM);
- la predisposizione e la comunicazione ai soggetti interessati, da parte del DIS, sentito il CISR tecnico, del modello contenente l'indicazione degli elementi utili alla descrizione dei beni ICT individuati negli elenchi predisposti ai sensi dell'articolo 7 del DPCM, nonché della individuazione delle informazioni necessarie ai fini della loro trasmissione che, ai sensi dell'articolo 1, comma 2, lettera b), del decreto-legge, deve avvenire entro sei mesi dalla comunicazione a ciascun soggetto dell'avvenuta inclusione nell'elenco di cui all'articolo 1, comma 2-*bis*, del decreto-legge (articolo 8, commi 1 e 2, del DPCM);
- l'adozione del decreto del Presidente del Consiglio dei ministri di cui all'articolo 1, comma 3, del decreto-legge, limitatamente alla previsione delle misure di sicurezza per la tutela delle informazioni relative all'elencazione dei soggetti, di cui all'articolo 5, comma 2, e dei beni ICT, di cui all'articolo 7, comma 2, lettera b), del DPCM.

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 n. 105/2019.

MODULARIO
P.C.M. 198

Mod. 251

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 dall'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 "decreto del Presidente del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, adottato in attuazione dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133", 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 "decreto del Presidente del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, adottato in attuazione dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

Roma,

Pres. Ermanno de Francisco