



Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici

Atto del Governo 240

Informazioni sugli atti di riferimento

Atto

	240	
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, della legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza	
Norma di delega:	Articolo 1, commi 3 e 4-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, della legge 18 novembre 2019, n. 133	
Numero di articoli:	11	
	Senato	Camera
Date:		
trasmissione	14/01/2021	14/01/2021
annuncio	14/01/2021	14/01/2021
assegnazione	14/01/2021	14/01/2021
termine per l'espressione del parere	13/02/2021	13/02/2021
Commissione competente	1 ^a (Affari Costituzionali),	I (Affari costituzionali) e IX (Trasporti)
Rilievi di altre Commissioni	4 ^a (Difesa), 5 ^a (Bilancio), 8 ^a (Lavori pubblici e comunicazioni) e 10 ^a (Industria, commercio, turismo)	V (Bilancio)

Contenuto

Lo schema di regolamento in esame è composto da **11 articoli** suddivisi in quattro Capi e due Allegati.

Il **Capo I**, recante Disposizioni generali, è composto dall'unico **articolo 1** che contiene le **definizioni** utilizzate nell'articolato.

Come esplicitato nella relazione illustrativa, l'articolo 1 reca soltanto le 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, nell'ottica di garantire la coerenza con l'assetto definitorio delineato dagli altri provvedimenti di attuazione del decreto-legge

Si richiamano, in particolare le seguenti definizioni:

- **soggetti inclusi nel perimetro** (lett. c): soggetti che siano stati individuati secondo le procedure di cui all'articolo 1, comma 2, lettera a), del decreto-legge 105/2019, e inclusi nell'elencazione contenuta nell'atto amministrativo adottato ai sensi dell'articolo 1, comma 2-bis, del medesimo decreto-legge;
- **rete, sistema informativo** (lett. e): 1) una rete di comunicazione elettronica ai sensi dell'articolo 1, comma 1, lettera dd), del decreto legislativo 259/2003 (ossia sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportata); 2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali, ivi inclusi i sistemi di controllo industriale; 3) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1 e 2), per il loro funzionamento, uso, protezione e manutenzione, compresi i

programmi di cui al punto 2);

- **servizio informatico** (lett. f): il servizio consistente interamente o prevalentemente nel trattamento di informazioni, per mezzo della rete e dei sistemi Informativi, ivi incluso quello di *cloud computing*;
- **bene ICT** (lett. g): (information and communication technology): insieme di reti, sistemi informativi e servizi informatici, o parti di essi, incluso nell'elenco di cui all'articolo 1, comma 2, lettera b), del decreto-legge 105/2019. Si tratta dell'elenco che i soggetti inclusi nel perimetro predispongono e aggiornano, con cadenza almeno annuale, recante i beni ICT di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono (art. 7 del DPCM 131/2020)
- **impatto sul bene ICT** (lett. i): limitazione della operatività del bene ICT, ovvero compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali. La definizione rileva ai fini dell'operatività della disposizione di cui all'articolo 1, comma 3, lettera a), del decreto-legge 105/2019, che impone l'obbligo di notifica al CSIRT italiano per gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui al comma 2, lettera b) del medesimo DL 105.

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

Si prevede, in sintesi, che - al verificarsi di uno degli incidenti elencati, aventi impatto in particolare su beni ITC - i soggetti inclusi nel perimetro sono tenuti a procedere alla notifica al CSIRT italiano (*Computer security incident response team*) tramite appositi canali di comunicazione entro 6 ore o entro 1 ora in base alla tipologia di incidente. Una volta definiti e avviati i piani di attuazione delle attività per il ripristino è data comunicazione al medesimo CSIRT italiano ed è trasmessa, se richiesta, una relazione tecnica sugli elementi significativi dell'incidente e sulle azioni adottate per porvi rimedio. Il DIS inoltra successivamente le notifiche ai competenti soggetti della struttura di governo. È altresì consentito, ai medesimi soggetti, di procedere ad una notifica su base volontaria di incidenti non ricompresi nell'elenco dello schema di decreto.

Più nel dettaglio, l'**articolo 2**, recante tassonomia degli incidenti, fa rinvio alle tabelle n. 1 e n. 2 dell'allegato A del provvedimento in esame che recano la **classificazione degli incidenti** aventi impatto sui beni ICT. Le due tabelle sono distinte 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.

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

Ai sensi dell'art. 1, comma 1, lett. g) per **bene ITC** ai fini dello schema di decreto in esame si intende un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, incluso nell'elenco del DL 105/2019. Per impatto sul bene ITC si intende (ai sensi dell'art. 1, comma 1, lett. i) una limitazione dell'operatività del bene ITC ovvero una compromissione della disponibilità, integrità o riservatezza dei dati e delle informazioni da esso trattati ai fini dello svolgimento della funzione o del servizio essenziali.

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

L'analisi di rischio è effettuata ai sensi dell'articolo 7, comma 2, del D.P.C.M. 30 luglio 2020, n. 131 recante Regolamento in materia di perimetro di sicurezza nazionale cibernetica, 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.

Tale previsione dispone che, una volta ricevuta la relativa comunicazione i soggetti inclusi nel perimetro, in **esito all'analisi del rischio**, per ogni funzione essenziale o servizio essenziale provvedono ad individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale. A tale fine sono valutati: 1) l'impatto di un incidente sul bene ICT, in termini sia di limitazione della operatività del bene stesso, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali; 2) le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione.

Riguardo alla formulazione del comma 2, *per declinare con maggiore chiarezza l'obbligo ivi previsto*, nel [parere del Consiglio di Stato](#) reso sullo schema in esame, si rappresenta l'opportunità di riformulare la disposizione nel seguente modo:

"I soggetti inclusi nel perimetro procedono alla notifica di cui al comma 1 anche nei casi in cui uno degli

incidenti individuati nelle tabelle di cui all'allegato A si verifichi a carico di un sistema informativo o un servizio informatico, o parti di essi, che condivide con un bene ICT funzioni di sicurezza, risorse di calcolo o memoria, ovvero software di base, quali sistemi operativi e di virtualizzazione".

Le **modalità della notifica** sono previste dal comma 3 che dispone che si proceda tramite appositi "*canali di comunicazione*" del CSIRT italiano aventi i requisiti previsti dal decreto legislativo n. 65 del 2018 (punto 1 lett. a) e secondo le **modalità definite dal CSIRT italiano** e rese disponibili sul sito Internet del CSIRT italiano secondo i **termini** ivi previsti.

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

I termini per la notifica sono così individuati:

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

Si tratta di incidenti consistenti, in base alla tabella 1, incidenti consistenti, in base alla tabella 2, in: guasto, infezione, installazione, movimenti laterali, azioni sugli obiettivi ivi elencati.

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

Si tratta di incidenti consistenti, in base alla tabella 2, in: azioni sugli obiettivi e disservizio ivi elencati.

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

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

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

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

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

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

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

Si prevede inoltre che le imprese che forniscono **reti pubbliche di comunicazioni** o servizi di **comunicazione elettronica** accessibili al pubblico (di cui all'articolo 16-ter, comma 2, del Codice delle comunicazioni elettroniche di cui al decreto legislativo n. 259 del 2003), con la notifica in questione,

comunicano che la stessa costituisce anche **adempimento dell'obbligo** previsto ai sensi dell'articolo 16-ter del Codice delle comunicazioni elettroniche (decreto legislativo n. 259 del 2003) e delle correlate disposizioni attuative.

In base all'art. 16-ter tali imprese sono tenute a:

- a) fornire al Ministero, e se necessario all'Autorità, le informazioni necessarie per valutare la sicurezza e l'integrità dei loro servizi e delle loro reti, in particolare i documenti relativi alle politiche di sicurezza; nonché;
- b) sottostare a una verifica della sicurezza effettuata dal Ministero, anche su impulso dell'Autorità, in collaborazione con gli Ispettorati territoriali del Ministero dello sviluppo economico, o da un organismo qualificato indipendente designato dal Ministero. L'impresa si assume l'onere finanziario della verifica.

Il Ministero e l'Autorità hanno la facoltà di indagare i casi di mancata conformità nonché i loro effetti sulla sicurezza e l'integrità delle reti.

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

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

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

I soggetti inclusi nel perimetro sono tenuti inoltre "ad assicurare che dell'avvenuta notifica sia fornita notizia all'articolazione per l'implementazione del perimetro prevista nell'ambito delle misure di sicurezza di cui all'allegato B (**sottocategoria 2.1.4 (ID.AM-6)**)".

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

Più in particolare la voce (sottocategoria) 2.1.4 (ID.AM-6) riguarda la definizione dei ruoli e delle responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (fornitori, clienti, partner).

Nel parere si chiede dunque che la disposizione – di cui all'art. 3 comma 8, così come all'art. 4 comma 4 - sia riformulata con una più esplicita e diretta indicazione dell'oggetto cui essa riferisce, alla quale potrà aggiungersi anche il rinvio alla corrispondente voce dell'allegato 2, non essendo sufficiente la mera indicazione del codice identificativo di tale voce (categoria e sottocategoria identificative della misura di sicurezza).

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

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

Si precisa, al comma 2, che le **notifiche volontarie** sono trattate dal CSIRT italiano **in subordine a quelle**

obbligatorie e qualora ciò non costituisca un "onere sproporzionato o eccessivo".

In ogni caso, la notifica volontaria "non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica".

Infine, come al comma 7 dell'art. 3, si prevede anche per le notifiche volontarie che i soggetti inclusi nel perimetro assicurano che dell'avvenuta notifica sia fornita notizia all'articolazione per l'implementazione del perimetro prevista nell'ambito delle misure di sicurezza di cui all'allegato B (sottocategoria 2.1.4 (ID.AM-6)).

Nel parere del Consiglio di Stato si evidenzia che occorre chiarire se la "notifica volontaria" debba essere effettuata attraverso gli stessi canali dedicati previsti per la notifica obbligatoria dall'articolo 3. Valuti inoltre l'Amministrazione se non sia preferibile e opportuno qualificare tale "notifica volontaria" con il diverso termine "informativa volontaria" o "comunicazione volontaria", eventualmente specificando modalità alternative e semplificate di comunicazione, posto che, come esplicitato nel comma 2, nessun obbligo ulteriore può derivare da tale iniziativa in capo al soggetto che effettua la comunicazione. 4.2. Il comma 3 deve essere riformulato nei seguenti, più semplici termini: "Dalla notifica volontaria non deriva alcun obbligo di ulteriori adempimenti a carico del soggetto notificante". 4.3. Vale per il comma 4 quanto considerato a proposito dell'articolo 3, comma 8. In alternativa, valuti l'Amministrazione se non riformulare il comma come segue: "Si applica il comma 8 dell'articolo 3".

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

Nel parere del Consiglio di Stato si evidenzia in proposito che manca nella sequenza logico-giuridica dell'articolato, così come costruito nello schema di d.P.C.M. in esame, il passaggio precedente e pregiudiziale, previsto nel periodo precedente della medesima lettera a) citata, in base al quale il "Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano, [che] inoltra tali notifiche, tempestivamente, al Dipartimento delle informazioni per la sicurezza anche per le attività demandate al Nucleo per la sicurezza cibernetica". È vero che il CISIRT italiano non è che un organismo interno al DIS (istituito ai sensi dell'articolo 8 del decreto legislativo n. 65 del 2018). Tuttavia, avendo la legge previsto espressamente questo passaggio (ancorché "interno"), si reputa corretto farne menzione, per completezza, anche nel regolamento. Occorre, dunque, inserire (valuti l'Amministrazione se nell'articolo 5 o precedentemente) una disposizione che attui (o, quanto meno, richiami) il predetto passaggio normativo, chiarendo che il CSIRT italiano (*Computer security incident response team*) trasmette immediatamente al DIS le notifiche ricevute.

Prima dell'attuale comma 2 deve essere quindi aggiunto il seguente comma "2. Le notifiche volontarie, di cui all'articolo 4, sono trasmesse solo nel caso in cui siano state trattate". L'attuale comma 2 diviene conseguentemente comma 3.

Il DIS inoltra altresì le **notifiche volontarie** di cui dell'articolo 4 nel caso in cui queste vengano trattate:

a) dal l'organo del **Ministero dell'interno** per la sicurezza e la regolarità dei servizi di telecomunicazione (previsto dall'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144);

b) dalla struttura della **Presidenza del Consiglio dei ministri** competente per la innovazione tecnologica e la digitalizzazione, qualora le stesse provengano da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, fatta eccezione per quelle concernenti i beni ICT in relazione ai quali per le attività di ispezione e verifica sono competenti le strutture specializzate di cui all'articolo 1, comma 6, lettera c), terzo periodo, del decreto-legge;

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

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

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

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

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

Il **Capo III** (articoli 7-11) **disciplina le misure di sicurezza**.

L'**articolo 7**, con cui inizia il Capo III, è rubricato proprio "Misure di sicurezza".

Tali misure, articolate in: **funzioni, categorie, sottocategorie, punti e lettere** sono individuate

nell'allegato B del decreto in questione.

L'insieme delle **misure, di carattere tecnico e organizzativo**, volte a garantire elevati livelli di sicurezza dei beni ICT sono riportate sistematicamente nel suddetto allegato e si integrano con gli ambiti già previsti dalla legislazione primaria.

Tra questi, a titolo esemplificativo vi sono quelli relativi: **"alla struttura organizzativa preposta alla gestione della sicurezza", "alle politiche di sicurezza e alla gestione del rischio", alla sicurezza fisica e logica e dei dati"**.

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

Nella relazione illustrativa si evidenzia che la scelta di adottare, quale punto di riferimento, il *Framework* nazionale ha consentito, tra l'altro, di addivenire ad un punto di equilibrio tra il livello prescrittivo, così come definito dal legislatore regolamentare e quello della concreta applicazione delle misure in questione che viene demandata a ciascun soggetto nell'ambito della rispettiva realtà organizzativa.

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

Per quanto concerne l'articolo 7 e la cosiddetta "legenda" dell'allegato 2 si ricorda che il Consiglio di Stato, nel parere reso, ha evidenziato l'opportunità, per una più agile lettura del testo, di inserire una più puntuale denominazione della rubrica dell'indice dell'allegato 2 in modo da chiarire che le funzioni sono costituite da macro-aree.

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

Nello specifico per i soggetti inclusi nel perimetro che debbono adottare, per ciascun bene ICT di rispettiva competenza, **le misure contenute nell'allegato B sono previsti due differenti termini temporali per l'adozione delle misure stesse: 6 mesi e 24 mesi.**

In particolare i termini sono distinti a seconda che si tratti di misure di più immediata attuazione o di misure per le quali l'implementazione richieda interventi maggiormente impegnativi sotto il profilo progettuale e programmatico.

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

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

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

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

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

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

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

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

L'articolo 9 è dedicato alla **tutela delle informazioni**.

In particolare, l'articolo in questione individua **nell'allegato C** del decreto in esame **le misure minime di sicurezza di natura tecnica e organizzativa che sono volte a tutelare le informazioni relative all'elenco dei soggetti inclusi nel perimetro, all'elenco dei beni ICT** e agli elementi delle notifiche di incidente.

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

Al fine di garantire in tempi celeri la tutela delle informazioni in questione, qualora queste ultime non richiedano particolari interventi da parte dei soggetti tenuti al loro rispetto, è previsto che **le disposizioni volte a tutelare la sicurezza delle informazioni stesse debbano essere applicate entro 60 giorni** dall'entrata in vigore del decreto in esame. Viene inoltre prevista **una clausola di salvaguardia per l'adozione da parte dei soggetti inclusi nel perimetro di ulteriori e più elevati livelli di sicurezza delle misure contenute nell'allegato B**.

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

L'articolo 10 precisa, al fine di assicurare una maggiore chiarezza tra le diverse norme ordinamentali di settore che **le misure di sicurezza** previste dal decreto in questione **non si applicano** all'elenco dei beni e citi delle reti, dei sistemi informativi dei sistemi informativi attinenti alla **gestione delle informazioni classificate**.

L'articolo 11, infine, precisa che dal decreto in questione **non devono derivare nuovi o maggiori oneri a carico della finanza pubblica**.

Presupposti normativi

Lo schema di decreto in esame è definito in attuazione delle previsioni del comma 3 dell'articolo 1 del decreto-legge 21 settembre 2019, n. 105, che demanda a un apposito **decreto del Presidente del Consiglio dei ministri**, da adottarsi su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR) entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto-legge, la definizione - con annessa disciplina dei termini e delle modalità attuative - delle **procedure** in base alle quali i soggetti inclusi nel perimetro di sicurezza nazionale cibernetica **notificano** al **Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT)** italiano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici inclusi nel perimetro e le misure volte a garantire elevati **livelli di sicurezza** delle reti, dei sistemi informativi e dei servizi informatici suddetti, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea.

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

Relativamente al **termine di adozione dello schema in esame**, come ricordato anche dal Consiglio di Stato nel parere espresso sul provvedimento, l'articolo 1, comma 3, del decreto-legge n. 105 del 2019 prevede che il decreto attuativo ivi previsto debba essere adottato "entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto" (ossia entro dieci mesi dal 21 novembre 2019, data di entrata in vigore della legge di conversione 18 novembre 2019, n. 133). Il termine sarebbe dunque venuto a scadenza il **21 ottobre 2020**. Tuttavia **l'articolo 103**, comma 1, del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, in considerazione dell'emergenza Covid-19, ha stabilito che "ai fini del computo dei termini ordinatori o perentori, propedeutici, endoprocedimentali, finali ed esecutivi, relativi allo svolgimento di procedimenti amministrativi su istanza di parte o d'ufficio, pendenti alla data del 23 febbraio 2020 o iniziati successivamente a tale data, non si tiene conto del periodo compreso tra la medesima data e quella del 15 aprile 2020". Successivamente, l'articolo 37 del decreto-legge legge 8 aprile 2020, n. 23, convertito, con modificazioni, dalla legge 5 giugno 2020, n. 40, ha prorogato il suddetto termine al 15 maggio 2020. Il Consiglio di Stato ha rilevato come ritenga che tale **periodo di sospensione** sia applicabile anche al **termine per l'adozione dei regolamenti**. "Ne consegue che il termine ultimo utile per l'adozione del decreto in esame deve ritenersi prorogato ex lege di 81 giorni (pari al periodo di sospensione, dal 23 febbraio al 15 maggio 2020)".

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

Nella premessa allo schema di decreto si richiama il vigente quadro normativo in materia di sicurezza cibernetica definito, da ultimo, dal decreto-legge n. 105 del 2019 e, in attuazione di questo, dal **DPCM n. 131 del 2020** in materia di **perimetro** di sicurezza cibernetica, dal [DPCM 8 agosto 2019](#) che ha dettato

disposizioni sul CSIRT italiano (*Computer security incident response team*).

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

Nelle premesse allo schema di decreto in esame si richiama altresì il [Framework nazionale per la cybersecurity e la data protection 2019](#) realizzato dal Centro di ricerca di *cyber intelligence and information security* (CIS) dell'Università La Sapienza di Roma e dal *Cybersecurity national lab* del Consorzio interuniversitario nazionale per l'informatica (CINI) con il supporto del DIS e del Garante per la protezione dei dati personali.

Si ricorda infine che gli interventi per il **rafforzamento delle infrastrutture legate alla protezione cibernetica** del Paese previste dal perimetro di sicurezza nazionale cibernetica (decreto-legge n. 105 del 2019), dalla direttiva NIS (attuata con il d.lgs. 65/2018) e dalle iniziative previste dalla strategia Europea di *Cybersecurity* del 16 dicembre 2020, inclusa l'applicazione del *Cybersecurity Act* (Regulation EU 2019/881) sono richiamati espressamente nello schema di **Piano nazionale di ripresa e resilienza** trasmesso al Parlamento nel gennaio 2021. In tale ambito si richiama l'obiettivo di "migliorare la resilienza dell'infrastruttura IT del nostro Paese, irrobustendo gli strumenti digitali e le competenze specialistiche necessari a garantire la continuità operativa partendo dalle funzioni e servizi essenziali dello Stato il cui malfunzionamento potrebbe creare un pregiudizio alla sicurezza nazionale ed europea". Lo stanziamento totale per questo progetto è di circa 1.250 milioni di euro, di cui circa 50 milioni già stanziati per la realizzazione di un *data center* del Ministero dell'Interno e per il potenziamento delle reti di connettività delle strutture operativi del CNVVF.

Senato: Dossier n. 354

Camera: Atti del Governo n. 240

21 gennaio 2021

Senato	Servizio Studi del Senato Ufficio ricerche su questioni istituzionali, giustizia e cultura	Studi1@senato.it - 066706-2451	 SR_Studi
Camera	Servizio Studi Dipartimento Istituzioni	st_istituzioni@camera.it - 066760-3855	 CD_istituzioni
	Servizio Studi Dipartimento Trasporti	st_trasporti@camera.it - 066760-2614	 CD_trasporti

La documentazione dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati è destinata alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. Si declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

AC0457