Senato della Repubblica
Camera dei deputati
XVIII Legislatura

Documentazione per l'esame di
Atti del Governo
-Profili finanziari-

Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici e misure volte a garantire elevati livelli di sicurezza

A.G. 240

2 marzo 2021

Informazioni sugli atti di riferimento

Natura atto:	Schema di decreto del Presidente del Consiglio dei ministri
Atto del Governo:	240
Titolo:	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 riferimento:	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
Relazione tecnica (RT):	presente

Finalità

Lo schema di decreto del Presidente del Consiglio dei ministri in esame reca il regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici[1] e di misure volte a garantire elevati livelli di sicurezza.

Il provvedimento è adottato ai sensi dell'art. 1, commi 3 e 4-*bis*, del DL n. 105/2019.

L'articolo 1 del DL n. 105/2019 ha istituito il Perimetro di sicurezza nazionale cibernetica (Perimetro) afferente alle reti, ai sistemi informativi e ai servizi informatici di amministrazioni pubbliche, enti ed operatori pubblici e privati rilevanti ai fini della sicurezza nazionale (comma 1). L'articolo 1 demanda ad un DPCM la definizione del sistema di notifica degli incidenti aventi impatto sul Perimetro (comma 3, lett. *a)*) nonché delle misure volte a garantire elevati livelli di sicurezza allo stesso (comma 3, lett. *b)*). Il suddetto schema di DPCM è trasmesso alla Camera dei deputati e al Senato della Repubblica per l'espressione del parere delle Commissioni parlamentari competenti per materia *(*comma 4-*bis)*. L'articolo 1, comma 18, del DL n. 105/2019 dispone, inoltre, che gli eventuali adeguamenti alle prescrizioni di sicurezza - definite ai sensi del medesimo articolo - delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici di cui al comma 1, siano effettuati con le risorse finanziarie disponibili a legislazione vigente.

Si evidenzia che alle norme ora descritte **non sono stati ascritti effetti sui saldi di finanza pubblica**. La relazione tecnica relativa al DL n. 105/2019, con riguardo alle medesime disposizioni, afferma che i relativi adempimenti verranno adottati dalle amministrazioni interessate in condizioni di neutralità finanziaria con le risorse finanziarie, umane e strumentali già previste a legislazione vigente.

Lo schema di decreto, composto di 11 articoli, è corredato di relazione tecnica.

Nella presente Nota sono riportati sinteticamente i contenuti delle disposizioni dello schema di decreto che presentano profili di carattere finanziario e le informazioni fornite dalla relazione tecnica [vedi tabella]. Vengono quindi esposti gli elementi di analisi e le richieste di chiarimento considerati rilevanti ai fini di una verifica delle quantificazioni riportate nella relazione tecnica.

[1] Di cui all'art. 1, comma 2, lett. b), del DL n. 105/2019.

Verifica delle quantificazioni

Disposizioni dello schema di Presidente del Consiglio dei ministri che presentano profili finanziari	Elementi forniti dalla relazione tecnica
Articoli da 1 a 6: recano le definizioni che rilevano ai fini del regolamento (articolo 1) e rinviano alle Tabelle 1 e 2 dell'allegato A per l'individuazione dei criteri di classificazione degli incidenti aventi impatto sui beni ICT (*information and comunication technology*) secondo un livello di gravità crescente (articolo 2). Vengono definite le procedure e i termini per la notifica degli incidenti di cui all'allegato A da parte dei soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica (amministrazioni pubbliche, enti ed operatori pubblici e privati rilevanti ai fini della sicurezza nazionale) al *Computer security incident response team* (CSIRT) italiano, istituito presso il Dipartimento informazioni e sicurezza (DIS) ai sensi dell'art. 8, comma 1, del D.lgs. n. 65/2018. La notifica avviene tramite appositi canali di comunicazione del CSIRT italiano, secondo modalità definite e rese disponibili sul proprio sito internet da parte del medesimo CSIRT. Sono oggetto di comunicazione allo stesso anche i piani di attuazione delle attività di ripristino dei beni ICT coinvolti nell'incidente oggetto di notifica (articolo 3). I soggetti del Perimetro possono notificare, su base volontaria, anche incidenti su beni ICT non indicati nell'allegato A (articolo 4). Le notifiche ricevute dal CSIRT italiano vengono dallo stesso trasmesse a diversi soggetti istituzionali individuati dalla norma. È prevista la possibilità di stipulare apposite intese con ciascuna delle amministrazioni interessate al fine di concordare le modalità di trasmissione delle notifiche (articolo 5). In materia di notifica di incidenti relativi a reti, sistemi informativi e servizi informatici attinenti alla gestione di informazioni classificate, resta fermo quanto previsto a legislazione vigente dalla legge n. 124/2007 (sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto) (articolo 6).	La relazione tecnica riferisce che le due tipologie di interventi previsti dal decreto (obblighi di notifica e obblighi di adozione di misure di sicurezza) non comportano nuovi o maggiori oneri per la finanza pubblica. Per quanto concerne gli obblighi di notifica (articoli da 2 a 6) la relazione tecnica precisa che al loro adempimento i soggetti pubblici inclusi nel "Perimetro" provvedono nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente. La notifica avverrà tramite appositi canali di comunicazione del CSIRT italiano aventi i requisiti di cui al punto 1, lett. *a)*, dell'allegato I, del D.lgs. n. 65/2018, secondo le modalità definite dal CSIRT italiano e rese disponibili sul proprio sito Internet che risulta già operativo. Il ricorso a tali canali di comunicazione - in quanto relativi al CSIRT italiano, già istituito presso il DIS con il citato decreto legislativo e successivamente disciplinato con il DPCM 8 agosto 2019 - **non comporta nuovi oneri o maggiori per la finanza pubblica**, atteso che all'implementazione dei suddetti canali si provvederà con le risorse finanziarie, umane e strumentali previste nei pertinenti capitoli del bilancio del DIS, dell'AISE e dell'AISI di cui all'art. 29 della legge n. 124/2007, già disponibili.
Articoli da 7 a 10: individuano le misure volte a garantire elevati livelli di sicurezza dei beni ICT. Tali misure hanno carattere tecnico e organizzativo, sono elencate sistematicamente nell'allegato B e – ai sensi dell'articolo 1, comma 3, lettera *b)*, del decreto legge n. 105/2019 – sono relative ad elementi quali: la struttura organizzativa preposta alla gestione	La **relazione tecnica** ribadisce il contenuto delle disposizioni e afferma che agli oneri che deriveranno dagli obblighi di adozione di misure di sicurezza si provvederà, come è stato precisato anche nella relazione tecnica allegata al decreto-legge, positivamente verificata dalla Ragioneria Generale dello Stato, a decorrere dagli esercizi finanziari 2020/2021, con le

della sicurezza, la protezione fisica e logica e dei dati, la formazione, l'integrità delle reti e di sistemi informativi ecc. La relazione illustrativa chiarisce che per l'individuazione delle misure, è stato assunto, quale base di riferimento, il "*Framework* nazionale per la *cybersecurity* e la *data protection*", edizione 2019. La premessa dell'allegato B, al punto 2 specifica che per ogni misura è fornita "una specifica più dettagliata dell'implementazione minima attesa, nonché delle modalità richieste al fine di descriverne l'adozione e dimostrarne l'attuazione" (articolo 7). Sono definite le modalità con le quali i soggetti inclusi nel perimetro debbano adottare, per ciascun bene ICT di rispettiva pertinenza, le misure di cui all'allegato B, nonché dei relativi termini entro i quali provvedere. In particolare, sono previsti due differenti termini di adozione delle misure, sei mesi e ventiquattro mesi, distinti, come precisato dalla relazione illustrativa, a seconda che si tratti di misure di più immediata attuazione, ovvero per la cui implementazione siano necessari interventi che richiedano una più impegnativa attività sotto i profili progettuali e programmatici. I termini sopra menzionati decorrono dalla data di trasmissione degli elenchi dei beni ICT predisposti da ogni singolo soggetto incluso nel perimetro (articolo 8). Sono individuate, nell'allegato C, le misure minime di sicurezza volte a tutelare le informazioni relative all'elenco dei soggetti inclusi nel perimetro, all'elenco dei beni ICT, agli elementi delle notifiche di incidente, al modello di cui all'articolo 8 recante le modalità di adozione delle misure di sicurezza e, infine, alla documentazione relativa alle misure di sicurezza adottate da parte dei soggetti inclusi nel perimetro ai sensi degli articoli 7 e 8. Tali misure devono trovare applicazione entro sessanta giorni dalla data di entrata in vigore delle norme in esame (articolo 9).	**risorse finanziarie, umane e strumentali disponibili a legislazione vigente**. La relazione tecnica precisa che l'avvenuta adozione delle misure di sicurezza e dei relativi aggiornamenti sarà comunicata mediante la piattaforma digitale costituita presso il DIS. L'utilizzo della piattaforma digitale, come indicato nella relazione tecnica al citato regolamento adottato con DPCM n. 131 del 2020, non comporta nuovi oneri a carico della finanza pubblica poiché al funzionamento della piattaforma istituita presso il DIS, si provvede con le risorse finanziarie, umane e strumentali previste nei pertinenti capitoli del bilancio del DIS, dell'Agenzia informazioni e sicurezza interna **(**AISE) e dell'Agenzia informazioni e sicurezza interna **(**AISI) di cui all'articolo 29 della legge 3 agosto 2007, n. 124, già disponibili. Per quanto concerne gli obblighi di adozione delle misure di sicurezza che i soggetti inclusi nel perimetro sono tenuti ad applicare, la relazione tecnica precisa che agli eventuali oneri si provvederà, a decorrere dagli esercizi finanziari 2020/2021, con le risorse finanziarie, umane e strumentali disponibili a legislazione vigente, così come sopra precisato con riferimento agli oneri derivanti dall'adozione delle misure di sicurezza sui beni ICT.
Articoli 11: prevede che all'attuazione del decreto in esame si provvede nei limiti delle risorse finanziarie, umane e strumentali disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.	La **relazione tecnica** ribadisce la previsione di invarianza finanziaria recata dalla norma.

In merito ai profili di quantificazione, si evidenzia preliminarmente che lo schema di regolamento in esame dà attuazione a quanto previsto dall'articolo 1 del DL n. 105/2019 che, nel disporre l'istituzione del "Perimetro di sicurezza nazionale cibernetica" - afferente alle reti, ai sistemi informativi e ai servizi informatici di amministrazioni pubbliche, enti ed operatori pubblici

e privati rilevanti ai fini della sicurezza nazionale - ha demandato ad un DPCM: la definizione del sistema di notifica al *Computer security incident response team* (CSIRT) italiano, già operativo presso il Dipartimento informazioni e sicurezza (DIS), degli incidenti aventi impatto sul Perimetro nonché la definizione, da parte dei soggetti del medesimo Perimetro, delle misure volte a garantire elevati livelli di sicurezza allo stesso.

I profili attuativi relativi al sistema di notifica e agli interventi da realizzare in tema di sicurezza dei beni ICT sono rispettivamente disciplinati dagli articoli da 2 a 6 e dagli articoli da 7 a 10. Le stesse norme sono, inoltre, assistite da una previsione di neutralità finanziaria (articolo 11) che nel ribadire quanto già previsto dall'art. 1, comma 18, del DL n. 105/2019, prevede che all'attuazione delle suddette disposizioni si provveda nei limiti delle risorse finanziarie, umane e strumentali disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica.

L'articolato in esame è completato da tre allegati: l'allegato A, cui fa rinvio l'articolo 2, recante la tassonomia degli incidenti, l'allegato B, previsto dall'articolo 7, che reca l'indicazione delle misure di sicurezza dei beni ICT e l'allegato C, indicato all'articolo 9, che individua le misure minime di sicurezza per la tutela delle informazioni.

Tanto premesso, con specifico riguardo al **sistema di notifica degli incidenti** (articoli da 2 a 6), pur considerato quanto affermato dalla relazione tecnica - che riferisce che la notifica avverrà tramite appositi canali di comunicazione predisposti dal CSIRT italiano alla cui implementazione si provvederà con le risorse previste nei pertinenti capitoli del bilancio del DIS, dell'AISE e dell'AISI, già disponibili - andrebbero forniti ulteriori dati ed elementi di valutazione volti a consentire la verifica della suddetta previsione di neutralità finanziaria. Ciò con riguardo alla generalità dei soggetti pubblici facenti parte del Perimetro della sicurezza nazionale cibernetica, che dovranno utilizzare i predetti canali di comunicazione.

Tali soggetti sembrerebbero infatti tenuti ad adottare in modo vincolante i suddetti canali e modelli di comunicazione, adeguandosi agli *standard* che individuerà il CSIRT. Il ricorso all'intesa, di cui all'articolo 5, quale strumento convenzionale attraverso il quale, eventualmente, concordare le modalità di trasmissione secondo modelli condivisi, stante il tenore letterale della disposizione, sembrerebbe essere di natura meramente facoltativa.

Anche per quanto riguarda le **misure di sicurezza,** definite ai sensi degli articoli da 7 a 10, si rileva che la copertura di eventuali oneri è disposta nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica come stabilito dal decreto legge n. 105/2019 e ribadito dall'articolo 11 del testo in esame. A tal proposito si rileva che le misure prevedono tra l'altro attività, a carattere periodico, quali esercitazioni, attività di formazione, potenziamento dei sistemi di sicurezza, che potrebbero comportare oneri non già previsti a legislazione vigente. Ciò posto, andrebbero forniti ulteriori elementi idonei a suffragare l'assunzione di invarianza finanziaria, tenendo conto, in particolare, che l'attuazione delle misure deve essere disposta nell'ambito di determinati intervalli temporali; pertanto andrebbe specificamente confermato l'effettivo allineamento, anche sotto un profilo temporale, delle risorse disponibili rispetto alle spese che si assume di dover sostenere per il perseguimento delle finalità previste dal decreto in esame.

In merito ai profili di copertura finanziaria, in considerazione del contenuto dell'articolo 11, volto esclusivamente ad affermare la neutralità sul piano finanziario delle norme contenute nello schema di decreto in esame, andrebbe valutata l'opportunità di riformularne la rubrica, sostituendo le parole: "Disposizioni finali" con le seguenti: "Clausola di invarianza finanziaria".

Tanto premesso, andrebbe peraltro valutata l'opportunità di sopprimere la clausola di invarianza medesima, poiché, trattandosi di un atto normativo di rango secondario, esso per sua natura non è suscettibile di determinare nuovi o maggiori oneri per la finanza pubblica. Su tale aspetto appare comunque necessario acquisire l'avviso del Governo.

Camera Servizio Bilancio dello Stato bs_segreteria@camera.it - 066760-2174 CD_bilancio

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.
VQAG240