DISPOSIZIONI URGENTI IN MATERIA DI PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA E DI DISCIPLINA DEI POTERI SPECIALI NEI SETTORI DI RILEVANZA STRATEGICA

Art. 1

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 attivita' civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, e' istituito il perimetro di sicurezza nazionale cibernetica. Entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la cybersicurezza (CIC):

a) sono definiti modalita' e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo; ai fini dell' individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla legge 3 agosto 2007, n. 124, si procede sulla base dei seguenti criteri:

1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attivita' civili, sociali o economiche fondamentali per gli interessi dello Stato;

2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici;

2-bis) l'individuazione avviene sulla base di un criterio di gradualita', tenendo conto dell'entita' del pregiudizio per la sicurezza nazionale che, in relazione alle specificita' dei diversi settori di attivita', puo' derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti;

b) sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualita' che tenga conto delle specificita' dei diversi settori di attivita', i criteri con i quali i soggetti

di cui al comma 2-bis predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della legge 3 agosto 2007, n. 124; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il Tavolo interministeriale di cui all'articolo 6 del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; entro sei mesi dalla data della comunicazione, prevista dal comma 2-bis, a ciascuno dei soggetti iscritti nell'elenco di cui al medesimo comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonche' quelli privati, di cui al citato comma 2-bis, trasmettono tali elenchi all'Agenzia per la cybersicurezza nazionale, anche per le attivita' di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza; il Dipartimento delle informazioni per la sicurezza, l'Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI) ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-bis, 4, 6 e 7 della legge n. 124 del 2007, nonche' l'organo del Ministero dell'interno per la sicurezza e per la regolarita' 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, accedono a tali elenchi per il tramite della piattaforma digitale di cui all'articolo 9, comma 1, del regolamento di cui al decreto del Presidente del Consiglio dei ministri n. 131 del 2020, costituita presso l'Agenzia per la cybersicurezza nazionale. L'elencazione dei soggetti individuati ai sensi del comma 2, lettera a), e' contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del CIC, entro trenta giorni dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al comma 2. Il predetto atto amministrativo, per il quale e' escluso il diritto di accesso, non e' soggetto a pubblicazione, fermo restando che a ciascun soggetto e' data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco. L'aggiornamento del predetto atto amministrativo e' effettuato con le medesime modalita' di cui al presente comma. Gli elenchi dei soggetti di cui alla lettera a) del comma 2 del presente articolo sono trasmessi al Dipartimento delle informazioni per la sicurezza, che provvede anche a favore dell'AISE e dell'AISI ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-bis, 4, 6 e 7 della legge 3 agosto 2007, n. 124. Entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, che disciplina altresi' i relativi termini e modalita' attuative, adottato su proposta del CIC:

a) sono definite le procedure secondo cui i soggetti di cui al comma 2-bis, notificano gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui al

comma 2, lettera b), al 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 attivita' demandate al Nucleo per la sicurezza cibernetica; il Dipartimento delle informazioni per la sicurezza assicura la trasmissione delle notifiche cosi' ricevute all'organo del Ministero dell'interno per la sicurezza e la regolarita' 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, nonche' alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato; (11)

b) sono stabilite misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera b), tenendo conto degli standard definiti a livello internazionale e dell'Unione europea, relative:

1) alla struttura organizzativa preposta alla gestione della sicurezza;

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

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

3) alla protezione fisica e logica e dei dati;

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

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

6) al monitoraggio, test e controllo;

7) alla formazione e consapevolezza;

8) all'affidamento di forniture di beni, sistemi e servizi di information and communication technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale, di standard e di eventuali limiti. 3-bis. Al di fuori dei casi di cui al comma 3, i soggetti di cui al comma 2-bis notificano gli incidenti di cui all'articolo 1, comma 1, lettera h), del regolamento di cui al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, aventi impatto su reti, sistemi informativi e servizi informatici di propria pertinenza diversi da quelli di cui al comma 2, lettera b), del presente articolo, fatta eccezione per quelli aventi impatto sulle reti, sui sistemi informativi e sui servizi informatici del Ministero della difesa, per i quali si applicano i principi e le modalita' di cui all'articolo 528, comma 1, lettera d), del codice di cui al decreto legislativo 15 marzo 2010, n. 66. I medesimi soggetti effettuano la notifica entro il termine di settantadue ore. Si applicano, per la decorrenza del termine e per le modalita' di notifica, in quanto compatibili, le disposizioni dell'articolo 3, comma 4, secondo e terzo periodo, del regolamento di cui al decreto del Presidente del Consiglio

dei ministri 14 aprile 2021, n. 81. Si applicano, altresi', le disposizioni di cui all'articolo 4, commi 2 e 4, del medesimo regolamento. Con determinazioni tecniche del direttore generale, sentito il vice direttore generale, dell'Agenzia per la cybersicurezza nazionale, e' indicata la tassonomia degli incidenti che debbono essere oggetto di notifica ai sensi del presente comma e possono essere dettate specifiche modalita' di notifica All'elaborazione delle misure di cui al comma 3, lettera b), provvedono, secondo gli ambiti di competenza delineati dal presente decreto, il Ministero dello sviluppo economico e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza. (11) Gli schemi dei decreti di cui ai commi 2 e 3 sono trasmessi 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 puo' essere comunque adottato. I medesimi schemi sono altresi' trasmessi al Comitato parlamentare per la sicurezza della Repubblica. L'atto amministrativo di cui al comma 2-bis e i suoi aggiornamenti sono trasmessi, entro dieci giorni dall'adozione, al Comitato parlamentare per la sicurezza della Repubblica. Per l'aggiornamento di quanto previsto dai decreti di cui ai commi 2 e 3 si procede secondo le medesime modalita' di cui ai commi 2, 3, 4 e 4-bis con cadenza almeno biennale. Con regolamento, adottato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, sono disciplinati le procedure, le modalita' e i termini con cui:

a) i soggetti di cui al comma 2-bis, che intendano procedere, anche per il tramite delle centrali di committenza alle quali essi sono tenuti a fare ricorso ai sensi dell'articolo 1, comma 512, della legge 28 dicembre 2015, n. 208, all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera b), appartenenti a categorie individuate, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, da adottare entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, ne danno comunicazione al Centro di valutazione e certificazione nazionale (CVCN), istituito presso il Ministero dello sviluppo economico; la comunicazione comprende anche la valutazione del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego. L'obbligo di comunicazione di cui alla presente lettera e' efficace a decorrere dal trentesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale della Repubblica italiana del decreto del Presidente del Consiglio dei ministri che, sentita l'Agenzia per la cybersicurezza nazionale, attesta l'operativita' del CVCN e comunque dal 30 giugno 2022. Entro quarantacinque giorni dalla ricezione della comunicazione, prorogabili di quindici giorni, una sola volta, in caso di particolare complessita', il CVCN puo' effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da

compiere anche in collaborazione con i soggetti di cui al comma 2-bis, secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Decorso il termine di cui al precedente periodo senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In caso di imposizione di condizioni e test di hardware e software, i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN. I test devono essere conclusi nel termine di sessanta giorni. Decorso il termine di cui al precedente periodo, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In relazione alla specificita' delle forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero dell'interno e del Ministero della difesa, individuati ai sensi del comma 2, lettera b), i predetti Ministeri, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, in coerenza con quanto previsto dal presente decreto, possono procedere, con le medesime modalita' e i medesimi termini previsti dai periodi precedenti, attraverso la comunicazione ai propri Centri di valutazione accreditati per le attivita' di cui al presente decreto, ai sensi del comma 7, lettera b), che impiegano le metodologie di verifica e di test definite dal CVCN. Per tali casi i predetti Centri informano il CVCN con le modalita' stabilite con il decreto del Presidente del Consiglio dei ministri, di cui al comma 7, lettera b). Non sono oggetto di comunicazione gli affidamenti delle forniture di beni, sistemi e servizi ICT destinate alle reti, ai sistemi informativi e ai servizi informatici per lo svolgimento delle attivita' di prevenzione, accertamento e repressione dei reati e i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni, sistemi e servizi ICT per le quali sia indispensabile procedere in sede estera, fermo restando, in entrambi i casi, l'utilizzo di beni, sistemi e servizi ICT conformi ai livelli di sicurezza di cui al comma 3, lettera b), salvo motivate esigenze connesse agli specifici impieghi cui essi sono destinati; (11)

b) i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici di cui al comma 2, lettera b), assicurano al CVCN e, limitatamente agli ambiti di specifica competenza, ai Centri di valutazione operanti presso i Ministeri dell'interno e della difesa, di cui alla lettera a) del presente comma, la propria collaborazione per l'effettuazione delle attivita' di test di cui alla lettera a) del presente comma, sostenendone gli oneri; il CVCN segnala la mancata collaborazione al Ministero dello sviluppo economico, in caso di fornitura destinata a soggetti privati, o alla Presidenza del Consiglio dei ministri, in caso di fornitura destinata a soggetti pubblici ovvero a quelli di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82; sono inoltrate altresi' alla Presidenza del Consiglio dei ministri le analoghe segnalazioni dei Centri di valutazione dei Ministeri dell'interno e della difesa, di cui alla lettera a); (11)

c) la Presidenza del Consiglio dei ministri, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del codice dell'Amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, di cui al comma 2-bis, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma, svolgono attivita' di ispezione e verifica in relazione a quanto previsto dal comma 2, lettera b), dal comma 3, dal presente comma e dal comma 7, lettera b), impartendo, se necessario, specifiche prescrizioni; nello svolgimento delle predette attivita' di ispezione e verifica l'accesso, se necessario, a dati o metadati personali e amministrativi e' effettuato in conformita' a quanto previsto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196; per le reti, i sistemi informativi e i servizi informatici di cui al comma 2, lettera b), connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, le attivita' di ispezione e verifica sono svolte, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonche', nei casi in cui siano espressamente previste dalla legge, in tema di prevenzione e di contrasto del crimine informatico, 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. (11) Nell'ambito dell'approvvigionamento di prodotti, processi, servizi ICT e associate infrastrutture destinati alle reti, ai sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera b), il CVCN assume i seguenti compiti:

a) contribuisce all'elaborazione delle misure di sicurezza di cui al comma 3, lettera b), per cio' che concerne l'affidamento di forniture di beni, sistemi e servizi ICT;

b) ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilita' note, anche in relazione all'ambito di impiego, definisce le metodologie di verifica e di test e svolge le attivita' di cui al comma 6, lettera a), dettando, se del caso, anche prescrizioni di utilizzo al committente; a tali fini il CVCN si avvale anche di laboratori dallo stesso accreditati secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri, adottato entro dieci mesi dalla data di entrata in vigore della legge di conversione del presente decreto, su proposta del CIC, impiegando, per le esigenze delle amministrazioni centrali dello Stato, quelli eventualmente istituiti, senza nuovi o maggiori oneri a carico della finanza pubblica, presso le medesime amministrazioni. Con lo stesso decreto sono altresi' stabiliti i raccordi, ivi compresi i contenuti, le modalita' e i termini delle comunicazioni, tra il CVCN e i predetti laboratori, nonche' tra il medesimo CVCN e i Centri di valutazione del Ministero dell'interno e del Ministero della difesa, di cui al comma 6, lettera a), anche la fine di assicurare il coordinamento delle rispettive attivita' e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesimi condizioni e livelli di rischio;

c) elabora e adotta, previo conforme avviso del Tavolo interministeriale di cui all'articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, schemi di certificazione cibernetica, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea, laddove, per ragioni di sicurezza nazionale, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica. I soggetti di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e quelli di cui all'articolo 16-ter, comma 2, del codice delle comunicazioni elettroniche di cui al decreto legislativo 1° agosto 2003, n. 259, inclusi nel perimetro di sicurezza nazionale cibernetica:

a) osservano le misure di sicurezza previste, rispettivamente, dai predetti decreti legislativi, ove di livello almeno equivalente a quelle adottate ai sensi del comma 3, lettera b), del presente articolo; le eventuali misure aggiuntive necessarie al fine di assicurare i livelli di sicurezza previsti dal presente decreto sono definite dall'Agenzia per la cybersicurezza nazionale;

b) assolvono l'obbligo di notifica di cui al comma 3, lettera a), che costituisce anche adempimento, rispettivamente, dell'obbligo di notifica di cui agli articoli 12 e 14 del decreto legislativo 18 maggio 2018, n. 65, e dell'analogo obbligo previsto ai sensi dell'articolo 16-ter del codice di cui al decreto legislativo 1° agosto 2003, n. 259, e delle correlate disposizioni attuative; a tal fine, oltre a quanto previsto dal comma 3, lettera a), anche in relazione alle disposizioni di cui all'articolo 16-ter del codice di cui al decreto legislativo 1° agosto 2003, n. 259, il CSIRT italiano inoltra le notifiche ricevute ai sensi del predetto comma 3, lettera a), autorita' nazionale competente NIS) di cui all'articolo 7 del decreto legislativo 18 maggio 2018, n. 65. Salvo che il fatto costituisca reato:

a) il mancato adempimento degli obblighi di predisposizione, di aggiornamento e di trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera b), e' punito con la sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000;

b) il mancato adempimento dell'obbligo di notifica di cui al comma 3, lettera a), nei termini prescritti, e' punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

c) l'inosservanza delle misure di sicurezza di cui al comma 3, lettera b), e' punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

d) la mancata comunicazione di cui al comma 6, lettera a), nei termini prescritti, e' punita con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

e) l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera b), in violazione delle condizioni o in assenza del superamento dei test imposti dal CVCN ovvero dai Centri di valutazione di cui al comma 6, lettera a), e' punito con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;

f) la mancata collaborazione per l'effettuazione delle attivita' di test di cui al comma 6, lettera a), da parte dei soggetti di cui al medesimo comma 6, lettera b), e' punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;

g) il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio dei ministri in esito alle attivita' di ispezione e verifica svolte ai sensi del comma 6, lettera c), e' punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000; (11)

h) il mancato rispetto delle prescrizioni di cui al comma 7, lettera b), e' punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000. L'impiego di prodotti e di servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici di cui al comma 2, lettera b), in assenza della comunicazione o del superamento dei test o in violazione delle condizioni di cui al comma 6, lettera a), comporta, oltre alle sanzioni di cui al comma 9, lettere d) ed e), l'applicazione della sanzione amministrativa accessoria della incapacita' ad assumere incarichi di direzione, amministrazione e controllo nelle persone giuridiche e nelle imprese, per un periodo di tre anni a decorrere dalla data di accertamento della violazione. Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attivita' ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attivita' ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, e' punito con la reclusione da uno a tre anni. All'articolo 24-bis, comma 3, del decreto legislativo 8 giugno 2001, n. 231, dopo le parole: "di altro ente pubblico," sono inserite le seguenti: "e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105,". Le autorita' competenti per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative sono la Presidenza del Consiglio dei ministri, per i soggetti pubblici e per i soggetti di cui all'articolo 29 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, di cui al comma 2-bis, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma.(11) Ai fini dell'accertamento e dell'irrogazione delle sanzioni amministrative di cui al comma 9, si osservano le disposizioni contenute nel capo I, sezioni I e II, della legge 24 novembre 1981, n. 689. Per i dipendenti dei soggetti pubblici di cui al comma 2-bis, la violazione delle disposizioni di cui al presente articolo puo' costituire causa di responsabilita' disciplinare e amministrativo-contabile. Le autorita' titolari delle attribuzioni di cui al presente decreto assicurano gli opportuni raccordi con il Dipartimento delle informazioni per la sicurezza e con l'organo del Ministero dell'interno per la sicurezza e la regolarita' dei servizi di telecomunicazione, quale autorita' di contrasto nell'esercizio delle attivita' di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito,

con modificazioni, dalla legge 31 luglio 2005, n. 155. (11) La Presidenza del Consiglio dei ministri, per lo svolgimento delle funzioni di cui al presente decreto puo' avvalersi dell'Agenzia per l'Italia Digitale (AgID) sulla base di apposite convenzioni, nell'ambito delle risorse finanziarie e umane disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica. (11) Al decreto legislativo 18 maggio 2018, n. 65, sono apportate le seguenti modificazioni:

a) all'articolo 4, comma 5, dopo il primo periodo e' aggiunto il seguente: «Il Ministero dello sviluppo economico inoltra tale elenco al punto di contatto unico e all'organo del Ministero dell'interno per la sicurezza e la regolarita' 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.»;(11)

b) all'articolo 9, comma 3, le parole «e il punto di contatto unico» sono sostituite dalle seguenti: «, il punto di contatto unico e l'organo del Ministero dell'interno per la sicurezza e la regolarita' 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,». Gli eventuali adeguamenti alle prescrizioni di sicurezza definite ai sensi del presente articolo, delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici di cui al comma 2-bis, sono effettuati con le risorse finanziarie disponibili a legislazione vigente. Per la realizzazione, l'allestimento e il funzionamento del CVCN di cui ai commi 6 e 7 e' autorizzata la spesa di euro 3.200.000 per l'anno 2019 e di euro 2.850.000 per ciascuno degli anni dal 2020 al 2023 e di euro 750.000 annui a decorrere dall'anno 2024. Per la realizzazione, l'allestimento e il funzionamento del Centro di valutazione del Ministero dell'interno, di cui ai commi 6 e 7, e' autorizzata la spesa di euro 200.000 per l'anno 2019 e di euro 1.500.000 per ciascuno degli anni 2020 e 2021. Il Presidente del Consiglio dei ministri coordina la coerente attuazione delle disposizioni del presente decreto che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del Dipartimento delle informazioni per la sicurezza, che assicura gli opportuni raccordi con le autorita' titolari delle attribuzioni di cui al presente decreto e con i soggetti di cui al comma 1 del presente articolo. Entro sessanta giorni dalla data di entrata in vigore del regolamento di cui al comma 6, il Presidente del Consiglio dei ministri trasmette alle Camere una relazione sulle attivita' svolte. (11) Nei casi in cui sui decreti del Presidente del Consiglio dei ministri previsti dal presente articolo e' acquisito, ai fini della loro adozione, il parere del Consiglio di Stato, i termini ordinatori stabiliti dal presente articolo sono sospesi per un periodo di quarantacinque giorni.

Versione in vigore dal 22 settembre 2022, non più in vigore dal 17 luglio 2024 · versione 17

RIFERIMENTI NORMATIVI

Atto	Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica
Estremi	Decreto-legge 21 settembre 2019, n. 105
Pubblicazione	Gazzetta Ufficiale del 21 settembre 2019

NOTE DI AGGIORNAMENTO

(11) Il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, ha disposto (con l'art. 16, comma 5) che "Nel decreto-legge perimetro ogni riferimento al Dipartimento delle informazioni per la sicurezza, o al DIS, ovunque ricorra, e' da intendersi riferito all'Agenzia per la cybersicurezza nazionale, fatta eccezione per le disposizioni dell'articolo 1, commi 2, lettera b), e 2-ter, del medesimo decreto-legge perimetro, e ogni riferimento al Nucleo per la sicurezza cibernetica e' da intendersi riferito al Nucleo per la cybersicurezza". Ha inoltre disposto (con l'art. 16, comma 6, lettera a)) che nel presente decreto-legge ogni riferimento al Ministero dello sviluppo economico e alla Presidenza del Consiglio dei ministri, ovunque ricorra, e' da intendersi riferito all'Agenzia per la cybersicurezza nazionale.

Fonte del testo: dati aperti ufficiali, licenza CC BY 4.0
Fonti e licenze su iuspedia.it/fonti-e-metodologia. Il testo non ha carattere di ufficialità: fa fede quello pubblicato nella Gazzetta Ufficiale.

Documento generato da Iuspedia.it il 25 novembre 2026
https://www.iuspedia.it/disposizioni-urgenti-in-materia-di-perimetro-di-sicurezza-nazionale/art-1-perimetro-di-sicurezza-nazionale-cibernetica/versione/17

Inquadra il QR code per aprire la pagina su Iuspedia.it