SENATO DELLA REPUBBLICA
XVIII LEGISLATURA

Doc. XXVII
n. 24

RELAZIONE

SULLE ATTIVITÀ SVOLTE PER L'ATTUAZIONE DELLE DISPOSIZIONI CHE DISCIPLINANO IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

(Articolo 1, comma 19-bis, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133)

Presentata dal Presidente del Consiglio dei ministri
(DRAGHI)

Comunicata alla Presidenza l'8 luglio 2021

PAGINA BIANCA

RELAZIONE AL PARLAMENTO SULL'ATTUAZIONE DEL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, dispone, all'articolo 1, comma 19-bis, che il Presidente del Consiglio dei ministri, entro 60 giorni dall'entrata in vigore del regolamento di cui all'articolo 1, comma 6, trasmetta al Parlamento una relazione sull'attuazione del perimetro di sicurezza nazionale cibernetica (PSNC).

Alla luce dell'entrata in vigore, l'8 maggio 2021, del suddetto regolamento di cui al DPR 5 febbraio 2021, n. 54, la presente relazione intende informare sulle attività svolte ai sensi della citata norma.

A tal fine, la descrizione dello stato di attuazione è stata effettuata senza tener conto delle modifiche da ultimo apportate all'architettura PSNC dal decreto-legge 14 giugno 2021, n. 82, "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" (sinteticamente descritte nella sezione conclusiva della relazione). Ciò in quanto il d.l. n. 82/2021 è ancora nella fase di conversione in legge e, in ogni caso, dispone solo un adeguamento della normativa perimetro agli attori governativi stabiliti nel nuovo assetto istituzionale, senza modificare la disciplina sostanziale.

PREMESSA – IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Il decreto-legge n. 105/2019, istitutivo del perimetro di sicurezza nazionale cibernetica, si pone l'obiettivo di evitare, mediante misure di carattere tecnico, procedurale e sul piano degli approvvigionamenti, pregiudizi per la sicurezza nazionale in ambito cibernetico mirando, in quest'ottica, ad un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale dello Stato.

Precisamente, sono oggetto di tutela le reti, i sistemi informativi e i 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 o 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, interruzione, anche parziali, o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Il PSNC è, pertanto, un perimetro di beni ICT.

Questi beni sono individuati tra le reti, i sistemi informativi e i servizi informatici di pertinenza dei soggetti inclusi nel PSNC e funzionali allo svolgimento del servizio o della funzione essenziale esercitata dal soggetto perimetro. Pertanto, in primo luogo, sono individuati i soggetti con le relative funzioni e i servizi essenziali e, successivamente, i soggetti provvedono ad identificare i beni ICT di pertinenza da includere nel perimetro.

Nello specifico, come detto, i soggetti sono individuati tra le amministrazioni pubbliche, gli enti o gli operatori pubblici o privati con sede nel territorio nazionale che esercitano funzioni essenziali dello Stato o prestano servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato[1], in modalità dipendenti dall'utilizzo di reti, sistemi

[1] Lo svolgimento da parte di un soggetto di una funzione o di un servizio essenziale è valutato dalle amministrazioni competenti per settore sulla base dell'ambito definito dall'articolo 2 del DPCM n. 131/2020, come indicato più nel dettaglio nel prosieguo della relazione.

informativi e servizi informatici e diventano soggetti perimetro solo in seguito all'inclusione nel relativo atto amministrativo del Presidente del Consiglio dei ministri.

Quest'ultimo è adottato ad esito del seguente procedimento: le amministrazioni competenti per ciascuno degli 11 settori definiti nel DPCM 30 luglio 2020, n. 131, predispongono delle liste di soggetti individuabili, che sono trasmesse al CISR tecnico per la relativa istruttoria e la successiva sottoposizione al Comitato interministeriale per la sicurezza della Repubblica (CISR). Dunque, il CISR formula la proposta formale per l'approvazione e la firma dell'atto amministrativo da parte del Presidente del Consiglio dei ministri. In seguito, il Dipartimento delle informazioni per la sicurezza (DIS) notifica ai soggetti la loro inclusione nel perimetro, entro trenta giorni dall'avvenuta iscrizione.

Tali soggetti procedono, dunque, all'individuazione dei propri beni ICT da inserire nel perimetro e li comunicano al DIS, entro 6 mesi dalla ricezione della notifica. All'esito di questo processo, essi sono tenuti ad implementare, sui beni ICT perimetro di propria pertinenza, secondo le tempistiche stabilite dalla normativa di attuazione, gli obblighi definiti dal decreto-legge.

Difatti, considerato che i beni ICT perimetro sono direttamente funzionali alla preservazione della sicurezza nazionale, è chiaro che questi devono essere sottoposti a misure, cautele e attenzioni maggiori rispetto a quelle eventualmente adottate dal soggetto sui beni informatici da esso utilizzati per attività non inerenti alla funzione o al servizio essenziale. Per questa ragione, la normativa individua direttamente le misure da attuarsi sui beni ICT perimetro, strutturandole in tre pilastri:

1. notifica degli incidenti cibernetici al CSIRT;
2. adozione delle misure di sicurezza stabilite dalla normativa di attuazione;
3. sottoposizione di beni, servizi informatici o sistemi informativi, che un soggetto perimetro intende acquisire per l'utilizzo sui beni ICT del perimetro, ad uno "scrutinio tecnologico" mirato a verificarne l'affidabilità.

In tale cornice, il rispetto dei suddetti obblighi viene verificato attraverso un'attività di vigilanza da parte della Presidenza del Consiglio dei ministri, del Ministero dello sviluppo economico e delle strutture specializzate del Ministero dell'interno e del Ministero della difesa, secondo gli ambiti di rispettiva competenza.

In caso di inottemperanza, il decreto-legge stabilisce un regime sanzionatorio che, a seconda del tipo di violazione, prevede delle sanzioni amministrative pecuniarie (che possono variare tra gli euro 200.000 e 1.800.000 in base al tipo di inadempimento), sanzioni amministrative accessorie e sanzioni di natura penale.

Il decreto-legge dispone anche in merito al coordinamento del perimetro con la disciplina sul Golden Power in ambito 5G. Infatti, le acquisizioni – a qualsiasi titolo – di beni, servizi e componenti relativi alla progettazione, alla realizzazione, alla manutenzione e alla gestione delle reti inerenti i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G ovvero di componenti ad alta intensità tecnologica funzionali alla predetta realizzazione o gestione, quando posti in essere con soggetti esterni all'UE, sono soggette ad un obbligo di notifica sia al CVCN, per lo svolgimento dello "scrutinio tecnologico" finalizzato alla verifica di eventuali vulnerabilità nelle predette tecnologie, sia alla della Presidenza del Consiglio dei ministri ai fini di un eventuale esercizio del potere di veto o l'imposizione di specifiche prescrizioni o condizioni.

Infine, il decreto-legge n. 105/2019 stabilisce il potere per il Presidente del Consiglio dei ministri, in caso di crisi cibernetica, di disattivare (ove indispensabile e per il tempo strettamente necessario) apparati o prodotti in caso di rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici.

ATTUAZIONE DEL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

Dall'entrata in vigore del decreto-legge n. 105/2019, notevoli sforzi sono stati profusi per raggiungerne la piena attuazione. A tal riguardo, è stato necessario porre in essere un'attività di definizione normativa e di creazione delle infrastrutture digitali funzionali all'interazione con i soggetti, alla comunicazione dei beni ICT e all'operatività del perimetro. Pertanto, a partire da novembre 2019, come determinato dal CISR e nell'ambito del CISR tecnico, sono stati avviati 6 Gruppi di lavoro ed alcuni relativi sottogruppi i cui lavori, caratterizzati da un'intensa e articolata attività di coordinamento interministeriale, affidata al DIS, si sono concretizzati in oltre 160 riunioni. Alla luce di tali sforzi, nonostante le difficoltà determinate dall'attuale crisi pandemica, è stato possibile, in tempi adeguati anche considerando le procedure previste per l'emanazione dei regolamenti attuativi – due dei quali (il DPCM n. 131/2020 e il DPCM n. 81/2021) sottoposti anche al parere delle competenti Commissioni parlamentari – definire gli elementi costitutivi del perimetro ed avviare la prima fase di operatività dello stesso.

A tal riguardo, fondamentale importanza ha rivestito la proficua collaborazione inter istituzionale, in particolare tra le amministrazioni competenti per settore e il DIS che, ai sensi dell'articolo 1, comma 19-bis del decreto, supporta il Presidente del Consiglio dei ministri nel coordinamento della coerente attuazione delle disposizioni del PSNC.

Le attività finora svolte si sono focalizzate prevalentemente sui seguenti ambiti:

1. definizione della normativa di attuazione, che include quattro decreti del Presidente del Consiglio dei ministri e un decreto del Presidente della Repubblica;
2. individuazione dei soggetti inclusi nel PSNC;
3. definizione dei beni ICT perimetro;
4. coordinamento tra le amministrazioni coinvolte attraverso il Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica.

1. Definizione della normativa di attuazione

Il decreto-legge prevede, per il completamento del quadro giuridico in esame, l'approvazione di 5 decreti, di cui quattro regolamenti da adottarsi con DPCM e un regolamento da adottare con DPR. Pertanto, significativa attenzione è stata rivolta al processo di definizione della normativa di dettaglio che ha portato all'entrata in vigore di 3 provvedimenti attuativi.

NORMA ATTUATIVA DEL D.L. 105/2019	OGGETTO	STATO
DPCM 30 luglio 2020, n. 131 – Regolamento in materia di perimetro di sicurezza nazionale cibernetica ai sensi dell'articolo 1, comma 2	• Criteri per l'identificazione dei soggetti da includere nel perimetro • Criteri per l'individuazione dei "beni ICT perimetro"	Pubblicato in G.U. 21 ottobre 2020

DPCM 14 aprile 2021, n. 81 – 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)* e di misure volte a garantire elevati livelli di sicurezza, in attuazione dell'articolo 1, comma 3	• Procedure di notifica degli incidenti aventi impatto sui "beni ICT perimetro" al CSIRT • Misure volte a garantire elevati livelli di sicurezza dei "beni ICT perimetro"	Pubblicato in G.U. 11 giugno 2021
DPR 5 febbraio 2021, n. 54 – Regolamento recante attuazione dell'articolo 1, comma 6	• Procedure, modalità e termini di "scrutinio tecnologico" da parte del CVCN e dei CV • Criteri di natura tecnica per l'individuazione delle categorie, di beni, sistemi e servizi ICT a cui si applica la procedura di valutazione • Verifica e ispezione da parte delle autorità competenti ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi	Pubblicato in G.U. 23 aprile 2021
DPCM attuativo dell'articolo 1, comma 6, lettera *a)*	• Categorie di prodotti ICT sottoposti alle valutazioni del CVCN e dei CV in fase di procurement da parte dei soggetti perimetro	In via di pubblicazione in G.U.
DPCM attuativo dell'articolo 1, comma 7, lettera *b)*	• Accreditamento e raccordi tra CVCN, CV e laboratori	In attesa di parere del Consiglio di Stato

Tav. 1 – Sintesi e stato dei decreti attuativi del decreto-legge n. 105/2019

DPCM 30 luglio 2020, n. 131

Il primo decreto, attuativo dell'articolo 1, comma 2, è il **DPCM 30 luglio 2020, n. 131, entrato in vigore** in seguito alla pubblicazione sulla Gazzetta Ufficiale del 21 ottobre 2020. Questo ha definito, secondo un criterio di gradualità: i **settori** ai quali si applica la normativa e le amministrazioni per essi competenti; i concetti di **funzione e servizio essenziale**; i **criteri e le modalità di individuazione dei soggetti perimetro**; il procedimento per **l'individuazione e la comunicazione dei beni ICT** da includere nello stesso.

In particolare, l'utilizzo del "**criterio di gradualità**" come parametro definitorio comporta che, nel corso delle fasi di implementazione successive a quella di "prima applicazione" del PSNC, potranno essere individuati ulteriori settori, soggetti e categorie di beni ICT da includere nel perimetro, in corrispondenza con una progressiva espansione dello stesso, come recentemente effettuato con

l'aggiornamento dell'elenco dei soggetti perimetro di giugno 2021 (illustrato più nel dettaglio nel prosieguo).

In tale ottica, in via prioritaria e "fatta salva l'estensione ad altri settori in sede di aggiornamento", sono stati individuati i seguenti **settori e le relative amministrazioni competenti**:

SETTORI	AMM.NI COMPETENTI
Governativo	Amministrazioni CISR
Interno	Ministero dell'interno
Difesa	Ministero della difesa
Spazio e aerospazio	Presidenza del Consiglio dei ministri, ai sensi della legge 11 gennaio 2018, n. 7
Energia	Ministero della transizione ecologica (in seguito al trasferimento della competenza dal Ministero dello sviluppo economico)
Telecomunicazioni	Ministero dello sviluppo economico
Economia e finanza	Ministero dell'economia e delle finanze
Trasporti	Ministero delle infrastrutture e della mobilità sostenibili
Servizi digitali	Ministero dello sviluppo economico, in raccordo con la struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione
Tecnologie critiche	Struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione , Ministero dello sviluppo economico e Ministero dell'università e della ricerca
Enti previdenziali e del lavoro	Ministero del lavoro e delle politiche sociali

Tav. 2 – Settori individuati dall'articolo 3 del DPCM n. 131/2020 e amministrazioni competenti per settore

Nell'ambito di tali settori, sono individuati i soggetti che esercitano le funzioni e i servizi essenziali oggetto di tutela, secondo la definizione dell'articolo 2 dello stesso DPCM, che stabilisce che:

- un soggetto esercita una funzione essenziale dello Stato quando l'ordinamento gli attribuisce compiti diretti 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.
- un soggetto presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato quando pone 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.

Anche per quanto riguarda l'**inclusione dei soggetti** nel PSNC, viene usato come parametro il criterio di gradualità e, pertanto, l'articolo 4 dispone che debbano essere individuati "in fase di prima

applicazione e fino all'aggiornamento del decreto" – tra i soggetti che svolgono le funzioni e i servizi essenziali per cui, in caso di interruzione o compromissione, il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime – i soggetti titolari delle funzioni e dei servizi essenziali **un'interruzione delle cui attività comporterebbe il mancato svolgimento della funzione o del servizio**.

Allo stesso modo, in relazione all'individuazione dei **beni ICT perimetro** sono individuate le reti, i sistemi informativi e i servizi informatici 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 dell'integrità o della riservatezza dei dati e delle informazioni**. Questi beni ICT sono individuati da ciascun soggetto perimetro che, all'esito di un'analisi del rischio per ogni funzione o servizio essenziale di pertinenza, individua i beni ICT impiegati per svolgere tale funzione o servizio essenziale, valutando:

- l'impatto di un incidente su tali beni ICT, in termini sia di limitazione della loro operatività, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da essi trattati, ai fini dello svolgimento della funzione o del servizio essenziali;
- le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, compresi quelli utilizzati per fini di manutenzione e gestione.

I soggetti sono tenuti a comunicare l'elenco dei beni ICT di loro pertinenza, funzionali allo svolgimento della funzione o del servizio essenziale per cui sono stati inclusi, entro 6 mesi dalla notifica di inclusione nel perimetro.

DPCM 14 aprile 2021, n. 81

Il secondo è il **DPCM 14 aprile 2021, n. 81**, attuativo dell'articolo 1, comma 3, **entrato in vigore** in seguito alla pubblicazione in G.U. l'11 giugno 2021. Questo definisce le modalità di **notifica degli incidenti** aventi impatto sui beni ICT perimetro al CSIRT e le **misure volte a garantire elevati livelli di sicurezza**.

Il decreto individua **i tipi di incidenti cibernetici per i quali è obbligatoria la notifica al CSIRT**, dividendoli in due categorie sulla base della gravità dell'incidente stesso e stabilendo diverse tempistiche per la relativa notifica. Gli incidenti cibernetici che rientrano nei 19 tipi considerati meno gravi (categoria A) devono essere notificati al CSIRT entro 6 ore, mentre quelli che rientrano nei 6 tipi considerati più gravi (categoria B) entro un'ora, con l'obbligo di integrare tempestivamente quanto comunicato in caso di conoscenza di elementi aggiuntivi (salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa). Al contempo, è possibile notificare, su base volontaria, anche i tipi di incidenti non elencati nel decreto.

Nell'ottica di armonizzare gli obblighi in materia di incidenti cibernetici stabiliti dalla normativa vigente, è previsto che la notifica di un incidente impattante i beni ICT perimetro effettuata al CSIRT costituisca anche adempimento dell'obbligo notifica ai sensi del decreto legislativo 18 maggio 2018, n. 65 (disciplina NIS) e del decreto legislativo 1 agosto 2003, n. 259 (disciplina TELCO). Al fine di assicurare un coordinamento istituzionale, il CSIRT inoltra la notifica all'autorità competente NIS. Nella stessa ottica, il DIS inoltra le notifiche ricevute dal CSIRT all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, alla struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione (in caso di notifiche provenienti da soggetti pubblici o soggetti che forniscono servizi fiduciari qualificati o sono

gestori di posta elettronica certificata), nonché al Ministero dello sviluppo economico (in caso di soggetti privati). In questo modo, le suddette finalità di armonizzazione e coordinamento istituzionale sono soddisfatte e rafforzate.

Quest'obbligo diventerà effettivo a partire dal 1° gennaio 2022, mentre fino al 31 dicembre 2021 vi sarà una fase di "collaudo" del sistema di notifica, recependo quanto indicato dalle Commissioni Parlamentari in sede di parere.

Ulteriormente, il decreto individua **le misure di sicurezza che i soggetti sono tenuti ad implementare in relazione ai beni ICT perimetro**. Queste sono state definite utilizzando, quale base di riferimento, il "*Framework nazionale per la cybersecurity e la data protection*", edizione 2019. Quest'ultimo, a sua volta, fa riferimento ad altri autorevoli strumenti internazionali in materia ed è stato utilizzato, allo stesso modo, anche dalle autorità competenti NIS per l'adozione delle linee guida sulle misure di sicurezza per gli operatori di servizi essenziali nell'ambito del decreto legislativo 18 maggio 2018, n. 65. Le misure in parola concernono: la protezione per la gestione dei beni ICT; la governance della sicurezza cibernetica; la valutazione del rischio e la strategia per la gestione dello stesso; la protezione degli asset; il rilevamento degli eventi anomali; la risposta agli incidenti rilevati; il recupero dei dati.

Tra queste rilevano, a titolo esemplificativo, le misure concernenti la sicurezza dei dati digitali memorizzati che, se ricompresi in alcune categorie considerate sensibili, devono essere localizzati e/o trattati con infrastrutture fisiche e tecnologiche localizzate sul territorio nazionale. A questa regola possono fare eccezione, in recepimento di quanto indicato dalle Commissioni parlamentari in sede di parere, i dati digitali di backup (se opportunamente cifrati), che possono essere conservati anche al di fuori del territorio nazionale ma comunque entro i confini dell'UE. Un'ulteriore misura consiste nell'obbligo di istituire, nell'articolazione del soggetto, la figura dell'incaricato della gestione e dell'attuazione degli obblighi del perimetro, nonché di un referente tecnico, i cui nomi sono comunicati al DIS. Anche le misure di sicurezza sono suddivise in due categorie – A e B – e sono stabiliti diversi termini per la loro adozione. Per le misure della categoria A, i soggetti sono tenuti alla loro adozione entro un termine di 6 mesi dalla data di trasmissione degli elenchi dei beni ICT o dalla data dell'entrata in vigore del decreto, se la trasmissione è avvenuta prima di tale data. Per le misure della categoria B, il termine per l'adozione delle misure di sicurezza è di 30 mesi.

Infine, il decreto stabilisce delle misure di sicurezza da applicarsi per la tutela delle informazioni relative all'elencazione dei soggetti e dei beni ICT perimetro, alle notifiche di incidenti e all'adozione delle misure di sicurezza, da adottarsi entro 60 giorni dall'entrata in vigore del decreto.

DPR 5 febbraio 2021, n. 54

Il terzo atto normativo, attuativo dell'articolo 1, comma 6, è il **DPR 5 febbraio 2021, n. 54, entrato in vigore** l'8 maggio in seguito alla pubblicazione sulla Gazzetta Ufficiale del 23 aprile 2021. Questo regolamento definisce: procedure, modalità e termini di scrutinio tecnologico da parte del Centro di valutazione e certificazione nazionale (CVCN) e dei Centri di valutazione (CV); criteri di natura tecnica per l'individuazione delle categorie di beni, sistemi e servizi ICT che devono essere soggetti allo "scrutinio tecnologico"; le modalità per la verifica e l'ispezione del rispetto degli obblighi stabiliti dalla normativa perimetro.

Per quanto riguarda il procedimento di "scrutinio tecnologico", è stabilito l'obbligo per i soggetti perimetro di comunicare, prima dell'avvio della procedura di affidamento o, ove questa non sia prevista, prima della conclusione del contratto di fornitura, al CVCN o ai CV l'intenzione di acquisire beni, sistemi e servizi ICT da destinare all'utilizzo sui beni ICT inclusi nel perimetro. Il CVCN o i

CV, dunque, pongono in essere le necessarie verifiche e test e, all'esito degli stessi, possono definire eventuali condizioni e test di hardware e di software da inserire nelle clausole del bando di gara o del contratto, nonché eventuali prescrizioni di utilizzo dell'oggetto dell'affidamento. Le verifiche e i test sono effettuati rispetto alle categorie di beni ICT individuate da un DPCM attuativo, sulla base dei criteri individuati nel regolamento in parola.

Per quanto riguarda le attività di ispezione, controllo e irrogazione delle sanzioni, queste sono effettuate: dalla Presidenza del Consiglio dei ministri, per quanto riguarda i soggetti pubblici e i soggetti che forniscono servizi fiduciari qualificati o sono gestori di posta elettronica certificata; dal Ministero dello sviluppo economico, per quanto riguarda i soggetti privati; dalle strutture specializzate del Ministero dell'interno e del Ministero della difesa, per le attività di rispettiva competenza. Il controllo è posto in essere in relazione all'adempimento degli obblighi di: predisposizione, aggiornamento e trasmissione dell'elenco dei beni ICT perimetro; notifica al CSIRT degli incidenti cibernetici; adozione delle misure di sicurezza; comunicazione al CVCN; impiego di prodotti e servizi sui beni ICT perimetro in conformità alle prescrizioni del CVCN, dei CV o dei laboratori accreditati di prova (LAP); collaborazione per l'effettuazione delle attività di test da parte dei soggetti; osservanza delle prescrizioni formulate dalle autorità competenti all'esito delle attività di ispezione e verifica. All'esito delle stesse, le autorità competenti possono impartire le prescrizioni necessarie e, eventualmente, avviare il procedimento per l'applicazione delle sanzioni previste dal decreto-legge.

Nonostante l'avvenuta entrata in vigore del DPR nei tempi previsti, la sua piena attuazione sarà subordinata, con particolare riferimento al pilastro dello "scrutinio tecnologico" sui beni ICT, al funzionamento del CVCN, che è stato differito a causa del ritardo, dovuto alla pandemia di COVID-19, nell'indizione del concorso per la dotazione delle risorse umane necessarie per l'avvio dell'operatività e per il corretto funzionamento delle procedure di valutazione. In ragione di ciò, il d.l. n. 82/2021 prevede che le disposizioni di cui all'articolo 1, comma 6, saranno efficaci 30 giorni dopo la pubblicazione del decreto del Presidente del Consiglio dei ministri che, sentita l'ACN, attesta l'operatività del CVCN e, comunque, dal 30 giugno 2022.

Decreto recante regolamento attuativo dell'articolo 1, comma 6, lettera a)

Il quarto **decreto** è **attuativo dell'articolo 1, comma 6, lettera a)** e individua, sulla base dei criteri dettati nel DPR n. 54/2021, l'**elenco delle categorie di beni, sistemi e servizi ICT, oggetto di valutazione da parte del CVCN e dei CV** qualora i soggetti perimetro siano intenzionati ad acquisirli per l'impiego sui beni ICT perimetro. Essendo strettamente correlato al DPR, benché il DPCM sia stato approvato il 16 novembre dal CISR tecnico ed esaminato, con esito favorevole, dal CISR il 25 successivo, lo stesso è stato firmato solo di recente in quanto si attendeva la previa pubblicazione del DPR in Gazzetta Ufficiale. Dunque, lo stesso è stato firmato dal Presidente del Consiglio dei ministri il 15 giugno 2021 ed è **in attesa di pubblicazione in Gazzetta ufficiale**.

Decreto recante regolamento attuativo dell'articolo 1, comma 7, lettera b)

Il quinto **decreto, attuativo dell'articolo 1, comma 7, lettera b),** riguarda le modalità di **accreditamento dei CV e dei LAP e la gestione dei raccordi del CVCN con i LAP e i CV**. Questo definisce le procedure e i requisiti – professionali e strumentali – che i CV e i LAP devono avere per verificare, nell'ambito delle rispettive competenze, le condizioni di sicurezza e l'assenza di vulnerabilità note di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture strategiche, nonché di ogni altro operatore per cui sussiste un interesse nazionale. Inoltre, stabilisce un meccanismo per la gestione dei raccordi tra i diversi centri di scrutinio

tecnologico, anche al fine di assicurare il coordinamento delle attività e perseguire la convergenza e la non duplicazione delle valutazioni in presenza di medesime condizioni e livelli di rischio.

Questo testo è stato approvato dal CISR ed è **in attesa di parere del Consiglio di Stato**.

2. Individuazione dei soggetti inclusi nel PSNC

In seguito all'entrata in vigore del DPCM n. 131/2020, è stato definito, con decreto del Presidente del Consiglio dei ministri del 25 novembre 2020, su proposta del CISR, il primo elenco dei soggetti perimetro. Tale atto non è sottoponibile a pubblicazione e su di esso non è esercitabile il diritto di accesso.

Sulla base del procedimento stabilito all'articolo 5 del DPCM n. 131/2020, le amministrazioni competenti per ciascuno degli 11 settori definiti nel decreto hanno predisposto delle liste di soggetti individuabili per l'inclusione del perimetro, che sono state trasmesse al CISR tecnico per la relativa istruttoria e la successiva sottoposizione al CISR. Dunque, il CISR ha formulato la proposta formale per l'approvazione e la firma del sopra citato atto amministrativo da parte del Presidente del Consiglio dei ministri.

Il DIS ha notificato a questi soggetti, il 22 dicembre 2020, la loro inclusione. A partire da tale data, è iniziato a decorrere il termine di 6 mesi per la trasmissione, da parte di tali soggetti, dei beni ICT di rispettiva pertinenza da includere nel perimetro.

Da ultimo, è stato approvato un aggiornamento del suddetto elenco e, con decreto del Presidente del Consiglio dei ministri del 15 giugno 2021, sono stati inclusi nuovi soggetti, funzioni e servizi essenziali o variate le funzioni o i servizi di quelli già inclusi. In questo modo, è stato disposto un allargamento dell'ambito di applicazione del perimetro ad ulteriori soggetti pubblici e privati che esercitano, attraverso reti, sistemi informativi e servizi informatici, complessivamente 223 funzioni essenziali dello Stato ovvero erogano servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato. Allo stesso tempo, si è provveduto ad un affinamento di alcune funzioni e servizi essenziali già ricompresi nel perimetro. In tal modo, viene incrementato il livello di resilienza cibernetica degli attori maggiormente sensibili per la sicurezza nazionale.

Il 17 giugno 2021, il DIS ha provveduto a notificare agli stessi la relativa inclusione nel perimetro.

3. Definizione dei beni ICT inclusi nel perimetro

Come sopraindicato, ai sensi del DPCM n. 131/2020, i soggetti del perimetro, entro 6 mesi dalla ricezione della comunicazione di avvenuta iscrizione nello stesso, devono provvedere alla predisposizione e alla trasmissione degli elenchi dei propri beni ICT, comprensivi della relativa architettura e componentistica, necessari allo svolgimento della funzione essenziale o all'erogazione del servizio essenziale per i quali sono stati inclusi.

Tale attività si è conclusa di recente, con il decorrere del termine per la comunicazione – da parte dei soggetti inclusi nel perimetro lo scorso dicembre (esclusi quelli impattati dal suddetto aggiornamento di giugno 2021, per i quali sono rinnovati i termini in ragione della modifica della funzione o del servizio essenziale di riferimento) – dell'elenco dei beni ICT perimetro. È iniziata, così, la fase "operativa", con l'avvio del sistema di notifica degli incidenti e del processo di adozione delle misure di sicurezza.

Questo risultato è stato possibile anche grazie alle attività portate avanti dal DIS, che ha predisposto il modello ontologico e la piattaforma digitale necessari alla comunicazione dei beni ICT perimetro,

secondo quando disposto dagli articoli 8 e 9 del DPCM n. 131/2020, nonché dalle Amministrazioni proponenti che hanno assicurato un'efficace e valida sinergia con il Dipartimento. Il DIS, in questa fase, in un'ottica di attiva collaborazione pubblico-privato, ha, inoltre, fornito un'assidua assistenza tecnica ai soggetti per la corretta individuazione dei beni ICT, attraverso circa 220 interazioni tra videoconferenze e interlocuzioni varie.

Grazie ai suddetti sforzi, è stato ad oggi individuato l'insieme di beni ICT che costituiscono il primo nucleo del perimetro di sicurezza nazionale cibernetica. Quest'elenco deve essere aggiornato dai soggetti perimetro con cadenza almeno annuale.

4. Coordinamento tra le amministrazioni coinvolte attraverso il Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica

Il processo di attuazione del perimetro è stato portato avanti attraverso uno stretto coordinamento tra le Amministrazioni coinvolte, in particolare in sede di Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica. Il Tavolo interministeriale, previsto all'articolo 6 del DPCM n. 131/2020, è stato istituito a supporto del CISR tecnico per le funzioni istruttorie in relazione all'individuazione dei soggetti perimetro e per ogni altra attività attribuita dal decreto-legge al CISR o al CISR tecnico. Questo è presieduto da un vice direttore generale del DIS ed è composto da due rappresentanti di ciascuna amministrazione CISR, da un rappresentante per ciascuna delle due Agenzie del comparto intelligence, nonché da due rappresentanti degli altri Ministeri di volta in volta interessati, che sono chiamati a partecipare alle riunioni in relazione agli argomenti da trattare. Questo si riunisce periodicamente e almeno una volta ogni sei mesi.

Dall'istituzione del perimetro, il Tavolo interministeriale si è riunito in due occasioni, nel corso delle quali ha valutato l'andamento del processo di attuazione del PSNC, nonché le prospettive di aggiornamento dell'atto amministrativo del Presidente del Consiglio dei ministri del 25 novembre 2020. Tale attività, come illustrato, ha portato all'ampliamento dei soggetti inclusi nel perimetro dello scorso mese di giugno.

PROSSIME FASI

In questa prima fase di attuazione del perimetro, grazie all'assidua interazione tra tutte le Amministrazioni coinvolte, nonché al dialogo e al supporto tecnico fornito ai soggetti perimetro da parte del DIS e dalle amministrazioni competenti, è stata definita l'area del perimetro di sicurezza nazionale cibernetica e ha preso avvio la fase di transizione verso la piena operatività del PSNC.

I prossimi mesi saranno, pertanto, incentrati sul raggiungimento dell'integrale efficacia e applicazione della normativa di attuazione e l'implementazione dei tre pilastri assumerà importanza primaria. A tal fine, si valuterà l'andamento della fase sperimentale del sistema di notifica al CSIRT, l'adeguatezza delle misure di sicurezza stabilite, nonché la corretta ottemperanza alle stesse da parte dei soggetti. Ulteriormente, si lavorerà per rendere operativo il CVCN e attivare il procedimento di "scrutinio tecnologico".

Eventuali necessità di affinamento e miglioramento, ispirate alla volontà di garantire al Paese livelli di resilienza e sicurezza cibernetica sempre crescenti, nonché adeguate al rischio connesso all'evoluzione delle tecnologie, potranno essere recepite attraverso l'aggiornamento dei regolamenti attuativi del perimetro (che, ai sensi dell'articolo 1, comma 5, del d.l. n. 105/2019, è effettuato con cadenza almeno biennale) e la predisposizione di un Testo unico in materia, come suggerito dal Consiglio di Stato in sede di parere.

Le suddette attività si inseriranno, inoltre, nel più ampio sforzo finalizzato a consentire, ad esito della conversione in legge del d.l. n. 82/2021, il celere avvio e l'agevole trasposizione in seno all'Agenzia per la cybersicurezza nazionale (ACN) delle funzioni perimetro dallo stesso individuate. Infatti, in un'ottica di assicurare l'unicità istituzionale di indirizzo e di azione, spesso invocata dagli operatori coinvolti, nei confronti dei soggetti pubblici e privati interessati, vengono trasferite all'ACN le competenze relative al PSNC previamente esercitate dalla Presidenza del Consiglio dei ministri, dal Dipartimento delle informazioni per la sicurezza e dal Ministero dello Sviluppo economico, incluso il Centro di valutazione e certificazione nazionale. Allo stesso modo, ai fini della completa attuazione del PSNC, sarà rilevante la trasposizione di competenze al Comitato interministeriale per la cybersicurezza (CIC), che andrà ad esercitare le funzioni previamente attribuite al CISR in relazione all'architettura cyber; il trasferimento del CSIRT presso l'ACN, che è ridenominato CSIRT Italia; il trasferimento del Nucleo per la sicurezza cibernetica presso l'ACN, che è ridenominato Nucleo per la cybersicurezza.

Nel frattempo, considerato che il perimetro di sicurezza nazionale cibernetica è strettamente collegato all'evoluzione degli scenari e delle esigenze del Paese, ci si focalizzerà anche sul costante monitoraggio di eventuali esigenze di aggiornamento ed espansione del perimetro stesso, così da assicurare l'inclusione degli attori maggiormente sensibili per la sicurezza nazionale.

180270152260