ATTI PARLAMENTARI

XIX LEGISLATURA

CAMERA DEI DEPUTATI

Doc. **XXVII**
n. **1**

RELAZIONE

SULLO STATO DI ATTUAZIONE DEL DECRETO-LEGGE RECANTE DISPOSIZIONI URGENTI IN MATERIA DI CYBERSICUREZZA, DEFINIZIONE DELL'ARCHITETTURA NAZIONALE DI CYBERSICUREZZA E ISTITUZIONE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

*(Articolo 17, comma 10-*bis*, lettera* b*), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109)*

Presentata dal Presidente del Consiglio dei ministri

(MELONI)

Trasmessa alla Presidenza il 18 novembre 2022

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

sommario

Introduzione 5

Attuazione dell'architettura nazionale di cybersicurezza 6

1 Attori istituzionali 9
- Il Presidente del Consiglio dei ministri e l'Autorità delegata 10
- Il Comitato interministeriale per la cybersicurezza – CIC 12
- L'Agenzia per la Cvybersicurezza Nazionale 12

2 Strutturazione dell'agenzia per la Cybersicurezza Nazionale 15
- Attuazione della struttura organizzativa 16
- Attuazione dell'autonomia patrimoniale, contabile e finanziaria 18
- Attuazione del sistema di gestione del personale 18

3 L'attuazione delle funzioni dell'Agenzia per la Cybersicurezza Nazionale 22
- Strategia Nazionale di Cybersicurezza 23
- Funzioni ai sensi della normativa NIS (d. Lgs. N. 65/2018) 24
- Funzioni di certificazione della cybersicurezza 26
- Attuazione del Perimetro di Sicurezza Nazionale Cibernetica (PSNC) 26
- Attuazione delle funzioni relative alla normativa in materia di "poteri speciali" 28
- Attuazione delle funzioni relative al codice dell'amministrazione digitale e al cloud nazionale 28
- Attuazione delle funzioni per la sicurezza delle comunicazioni elettroniche 29
- Attuazione della funzione di preparazione, prevenzione, gestione e risposta a eventi cibernetici 30
- Mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza 30
- Relazioni e cooperazione internazionale 32
- Sviluppo di competenze e capacità industriali, tecnologiche e scientifiche 33
- Promozione della consapevolezza in materia di cybersicurezza 35
- Sviluppo della formazione e della crescita professionale 35
- Collaborazioni istituzionali 36

4 Il Nucleo per la Cybersicurezza - NCS 39

Conclusione 42

PAGINA BIANCA

introduzione

Il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109 (nel prosieguo "decreto-legge"), prevede, all'articolo 17, comma 10-bis, lettera b), che entro il 31 ottobre 2022 il Presidente del Consiglio dei ministri trasmetta alle Camere una relazione sullo stato di attuazione, al 30 settembre 2022, delle disposizioni di cui al medesimo decreto-legge, anche al fine di formulare eventuali proposte in materia.

La relazione in parola rappresenta un obbligo informativo "*una tantum*" verso il Parlamento, al fine di garantire un controllo del Legislatore sui risultati conseguiti con l'attuazione del decreto-legge n. 82 del 2021.

Con la presente Relazione si provvede, quindi, all'attuazione della norma sopra richiamata, dando conto delle attività poste finora in essere dall'Esecutivo per la realizzazione del nuovo impianto normativo disegnato dal Legislatore, anche al fine di individuare, alla luce dell'esperienza del primo anno di operatività, le eventuali problematicità e le misure per superarle[1].

La presente relazione avrà un contenuto prevalentemente normativo e descrittivo, focalizzandosi su come è stata articolata la struttura organizzativa e sono state avviate le attività da un punto di vista tecnico-funzionale.

[1] Considerato che la presente relazione precede di un mese la presentazione della Relazione annuale al Parlamento di cui all'articolo 14, comma 1, lett. a), del decreto-legge (che, ai sensi dell'articolo 17, comma 10-bis, è trasmessa, con riferimento alle attività del 2021, entro il 30 novembre 2022 invece che entro il 30 aprile), si ritiene opportuno precisare che la più dettagliata rendicontazione delle attività svolte sarà presentata nella Relazione annuale.

attuazione

Attuazione dell'Architettura Nazionale di Cybersicurezza

La previsione di una relazione sullo stato di attuazione del decreto-legge n. 82/2021, recante "*disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", a circa un anno e mezzo dall'adozione dello stesso, risulta particolarmente utile in considerazione del fatto che il decreto-legge ha profondamente ridisegnato l'architettura nazionale di cybersicurezza, istituendo nuovi attori istituzionali nell'ecosistema nazionale cyber e razionalizzando e armonizzando le competenze in materia di cybersicurezza ad essi attribuite.

Tale operazione si è resa necessaria per dotare il nostro Paese di un apparato istituzionale che riesca a contrastare, sotto tutti i fronti, i rischi generati dal processo di digitalizzazione della società come, ad esempio, lo sfruttamento da parte di filiere criminali o attori statuali delle vulnerabilità delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche, allo scopo di provocare il malfunzionamento o addirittura l'interruzione di funzioni essenziali dello Stato e di servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato. Difatti, la ridisegnata architettura istituzionale affianca al fondamentale ruolo delle attività di prevenzione e risposta al cyber-crime (di principale competenza delle Forze di polizia), della difesa e della sicurezza militare dello Stato nel dominio cibernetico (in capo al Ministero della difesa), della ricerca ed elaborazione informativa (di competenza degli Organismi di informazione per la sicurezza), quello delle attività volte alla tutela della sicurezza e della resilienza nello spazio cibernetico, istituendo un apposito ente – l'Agenzia per la cybersicurezza nazionale – con ruolo di Autorità nazionale in materia. Essa è, infatti, deputata alla tutela della sicurezza e della resilienza nello spazio cibernetico, anche ai fini della tutela della sicurezza nazionale, con il condiviso obiettivo di raggiungere un elevato livello di sicurezza nello spazio cibernetico per il sistema-Paese.

Il decreto-legge ha ridisegnato l'assetto competenziale definito dal DPCM 17 febbraio 2017 e aggiornato le funzioni in materia, a partire dal Vertice politico – che rimane il Presidente del Consiglio dei ministri – fino al livello tattico-tecnico, creando un sistema sinergico, al quale partecipano anche tutte le altre amministrazioni pubbliche, l'accademia, gli enti di ricerca e il settore privato, che concorrono a salvaguardare e promuovere la cybersicurezza nazionale.

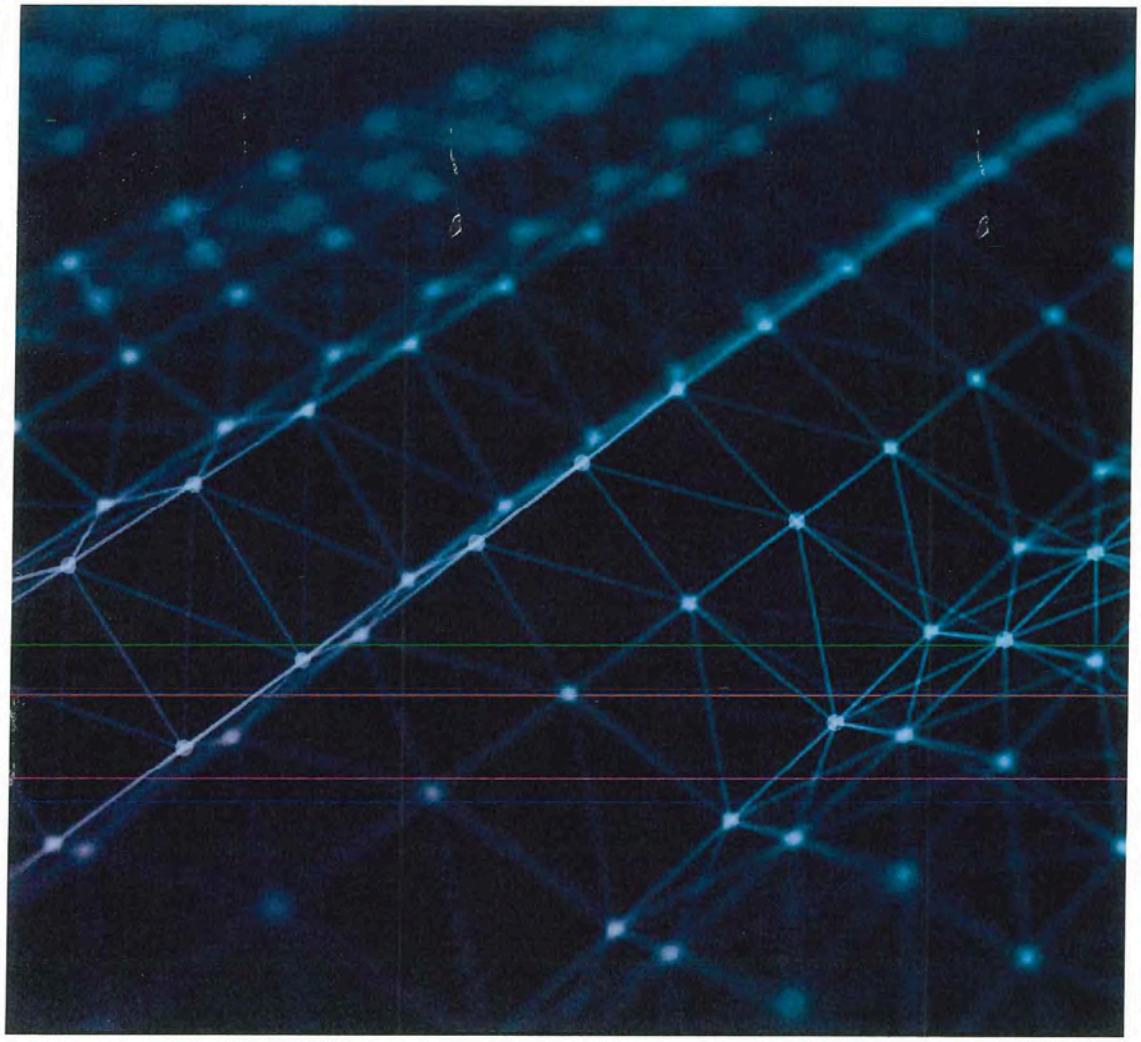
La riforma posta in essere con il decreto-legge ha, pertanto, avuto l'obiettivo di: attuare adeguate misure di cybersicurezza, intendendosi con tale termine, l'insieme delle attività necessarie per proteggere e assicurare la disponibilità, la confidenzialità e l'integrità di reti, sistemi informativi, servizi informatici e comunicazioni elettroniche dalle minacce informatiche, garantendone altresì la resilienza; porre la sicurezza e la resilienza cibernetiche a fondamento del processo di digitalizzazione del Paese in un contesto di piena sinergia pubblico-privato; promuovere la cultura della cybersicurezza; porre le basi formative in ambito *cyber*; perseguire una effettiva capacità di mantenere relazioni bilaterali e multilaterali e partecipare attivamente ai processi di definizione delle politiche, delle norme e degli *standard* internazionali in materia.

In virtù di tale significativo riassetto, l'attuazione della riforma ha richiesto, e ancora richiede, un rilevante numero di decreti attuativi (circa 40), la cui adozione è caratterizzata, in diversi casi, da un procedimento "aggravato". Difatti, anche in considerazione della speciale normativa che disciplina il funzionamento dell'Agenzia, il Legislatore ha voluto che il contenuto dei provvedimenti attuativi fosse frutto sia di un processo "condiviso" tra i diversi Ministeri aventi interessi, diretti o riflessi, nell'ambito della cybersicurezza, sia di una preventiva consultazione del Legislatore stesso. Pertanto, il procedimento di adozione di molti dei DPCM che si menzioneranno nel prosieguo prevede il coinvolgimento del Comitato interministeriale per la cybersicurezza, delle Commissioni parlamentari competenti e del Comitato Parlamentare per la sicurezza della Repubblica (COPASIR).

Tale requisito ha consentito che le numerose disposizioni adottate, su impulso anche dell'Agenzia, all'incipit della riformata architettura nazionale, siano il risultato della più ampia condivisione tra i diversi poteri dello Stato.

> *Al contempo, ciò ha comportato un allungamento dei tempi di definizione degli atti normativi relativi al funzionamento dell'Agenzia, che può non sempre perfettamente conciliarsi con le esigenze di rapidità della tutela della cybersicurezza e di conseguente adattamento dell'Agenzia stessa. Pertanto, andrebbe opportunamente ponderato un eventuale intervento volto a snellire le procedure di revisione dei suddetti decreti attuativi, specie in relazione a modifiche e/o aggiornamenti non strutturali.*

PAGINA BIANCA



1. ATTORI ISTITUZIONALI

Il Presidente del Consiglio dei ministri e l'Autorità delegata

L'unità e la coerenza di azione nella nuova architettura cyber è garantita, al vertice, dall'indirizzo politico-strategico fornito **dal Presidente del Consiglio dei ministri** e **dal Comitato interministeriale per la cybersicurezza - CIC**.

Al Presidente del Consiglio, l'articolo 2 del decreto-legge attribuisce in via esclusiva: l'alta direzione e la responsabilità generale delle politiche di cybersicurezza; l'adozione, sentito il CIC, della strategia nazionale di cybersicurezza, che rappresenta il principale documento programmatico che indica gli obiettivi che l'Italia si pone in relazione allo spazio cibernetico e gli strumenti per realizzarli; la nomina e la revoca del Direttore generale e del Vice Direttore generale dell'Agenzia.

L'alta direzione e la responsabilità delle politiche di cybersicurezza vengono principalmente realizzate mediante l'adozione delle direttive in materia e delle disposizioni necessarie per l'organizzazione e il funzionamento dell'Agenzia. Ciò è stato conseguito, anzitutto, mediante l'adozione di quattro regolamenti: il Regolamento di contabilità (DPCM 9 dicembre 2021, n. 222); il Regolamento di organizzazione e funzionamento (DPCM 9 dicembre 2021, n. 223); il Regolamento del personale (DPCM 9 dicembre 2021, n. 224); il Regolamento recante le procedure per la stipula di contratti di appalti di lavori, servizi e forniture per le attività dell'Agenzia per la cybersicurezza nazionale finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico (c.d. appalti in deroga), adottato dal Presidente del Consiglio il 1° settembre 2022. I quattro atti regolamentari saranno più volte citati nella presente Relazione, in quanto costituiscono i primi atti normativi con i quali è stata adottata la disciplina di dettaglio per l'attuazione del decreto-legge e costituiscono, pertanto, la principale base giuridica, insieme al decreto-legge, sulla quale l'Agenzia fonda la propria struttura.

La seconda competenza esclusiva del Presidente è l'adozione della strategia nazionale di cybersicurezza. Il Presidente del Consiglio ha adottato la Strategia nazionale di cybersicurezza 2022-2026, unitamente al relativo Piano di implementazione, con DPCM del 17 maggio 2022, dopo aver sentito, in pari data, il CIC.

La predisposizione della Strategia è, invece, uno dei compiti affidati dal decreto-legge all'Agenzia e alla sua definizione si è giunti a seguito di un percorso che ha visto la collaborazione di tutte le amministrazioni competenti, a guida ACN, di cui si dirà nel prosieguo in maniera più dettagliata.

Infine, la terza competenza esclusiva del Presidente del Consiglio è la nomina dei Vertici dell'Agenzia, avvenuta, per il Direttore generale, Roberto Baldoni, con DPCM 5 agosto 2021 – il giorno successivo alla conversione in legge del decreto-legge – e, per il Vice Direttore generale, Nunzia Ciardi, con DPCM 16 settembre 2021. La rapida nomina del Direttore generale dell'Agenzia e quella, immediatamente successiva, del Vice Direttore generale, cioè di coloro in possesso, tra le altre cose, del potere direttoriale organizzativo, ha indubbiamente dato un forte segnale sulla volontà di dare esecuzione immediata alle nuove disposizioni normative.

A completamento del quadro istituzionale, con il DPCM 13 settembre 2021, il Presidente del Consiglio dei ministri ha conferito la delega in materia di cybersicurezza al **Sottosegretario di Stato-Autorità delegata** per la sicurezza della Repubblica, Franco Gabrielli, trasferendogli le funzioni non attribuite al Presidente stesso in via esclusiva, mantenendo, in ogni caso, il potere di direttiva e la possibilità di avocare, in qualsiasi momento tutte o soltanto alcune di esse (articolo 3, comma 2, del decreto-legge).

Individuando l'Autorità delegata quale figura cui delegare i poteri nell'ambito della cybersicurezza, è stato creato un punto di raccordo tra le attività di sicurezza nazionale nello spazio cibernetico, proprie dell'Agenzia, e quelle nel campo delle attività di ricerca informativa, appartenenti invece all'*intelligence*[2].

Tale impostazione si è rivelata particolarmente funzionale, anche in virtù del previsto, diretto riferimento del Direttore generale all'Autorità politica, di cui si dirà nel prosieguo.

L'Autorità delegata ha, infatti, presieduto, ai sensi dell'articolo 116, comma 1, del Regolamento del personale, la Commissione *ad hoc* deputata all'inquadramento *una tantum* nei ruoli dell'Agenzia del personale messo a disposizione dal Dipartimento informazioni per la sicurezza - DIS.

L'Autorità delegata può, inoltre, convocare, su proposta del Direttore generale dell'Agenzia, e presiedere il **Comitato di Vertice**[3] di cui all'articolo 9 del Regolamento di organizzazione e funzionamento dell'Agenzia (DPCM 9 dicembre 2021 n. 223), nel cui ambito vengono trattate decisioni strategiche concernenti, tra l'altro, l'organizzazione e il funzionamento dell'Agenzia. Il Comitato di Vertice si è riunito per la prima volta il 14 giugno 2022 in relazione alla designazione dei componenti del Comitato tecnico-scientifico[4] e per quella dei componenti del Collegio dei revisori dei conti[5].

[2] Ai sensi dell'articolo 4 della legge 3 agosto 2007, n. 124, difatti, "il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono del DIS per l'esercizio delle loro competenze, al fine di assicurare piena unitarietà nella programmazione della ricerca informativa del Sistema di informazione per la sicurezza, nonché nelle analisi e nelle attività operative dei servizi di informazione per la sicurezza."

Il Comitato Interministeriale per la Cybersicurezza - CIC

Altro attore fondamentale nel quadro dell'architettura nazionale di cybersicurezza che compare per la prima volta nel panorama istituzionale è il **Comitato interministeriale per la cybersicurezza - CIC**, cui l'articolo 4 attribuisce funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. Il CIC è istituito presso la Presidenza del Consiglio dei ministri e rappresenta il momento di massimo raccordo politico in materia. Il Comitato, di cui il Direttore generale svolge la funzione di segretario, è presieduto dal Presidente del Consiglio ed è composto dall'Autorità delegata e dai dieci Ministri individuati specificamente dalla norma, con possibilità di invitare altri partecipanti in relazione alle questioni da trattare, ma senza diritto di voto.

Le rilevanti funzioni attribuite al CIC sono finora state esercitate in quattro occasioni, nel corso delle quali sedute sono stati posti al vaglio del Comitato: nella seduta del 9 dicembre, gli schemi dei tre regolamenti di contabilità, di organizzazione e funzionamento, e del personale dell'Agenzia[6]; nella seduta del 17 maggio, la Strategia nazionale di cybersicurezza[7] e il DPCM 18 maggio 2022, n. 92, recante il Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa (ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge 21 settembre 2019, n. 105 c.d. "decreto-legge perimetro")[8]; nella seduta del 28 luglio, il bilancio preventivo dell'Agenzia[9]; nella seduta del 1° settembre, il "Regolamento recante le procedure per la stipula di contratti di appalti di lavori, servizi e forniture per le attività dell'agenzia per la cybersicurezza nazionale finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico"[10].

Con l'approvazione dei suddetti provvedimenti, è stata vidimata la scelta, risultata vincente, di far supportare il Vertice politico da un apposito Comitato di Ministri che garantisca un raccordo inter istituzionale orizzontale, a livello politico-strategico, nella materia della cybersicurezza.

L'Agenzia per la Cybersicurezza Nazionale

Tra le principali novità introdotte dal decreto-legge, vi è la menzionata istituzione – ai sensi dell'articolo 5 – dell'Agenzia per la cybersicurezza nazionale (ACN) di cui si avvalgono il Presiden-

[3] Il Comitato di Vertice è presieduto dal Presidente del Consiglio dei ministri, ovvero dall'Autorità delegata, ove istituita, che ne dispone la convocazione, ove ritenuta opportuna, ed è composto dal Direttore generale e dal Vice Direttore generale. Il Capo di Gabinetto dell'Agenzia ne svolge le funzioni di segretario.
[4] Vedasi il combinato disposto articolo 7, comma 1-bis, d.l. n. 82/2021 e articolo 11, comma 4, DPCM 223 del 2021
[5] Articolo 7 del DPCM 223 del 2021.

te del Consiglio dei ministri e l'Autorità delegata per la sicurezza della Repubblica, ove istituita, per l'esercizio delle specifiche competenze in materia di cybersicurezza.

L'Agenzia è un ente di diritto pubblico, dotato di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, posto a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

I continui contatti tra i Vertici dell'Agenzia, da un lato, e il Presidente del Consiglio dei ministri e l'Autorità delegata, dall'altro, nonché la partecipazione, con le funzioni di segretario, del Direttore generale dell'ACN al CIC, hanno consentito l'immediata traduzione della direzione politica in linee di azione concrete. L'assenza di figure intermedie tra il Vertice politico in materia di politiche di cybersicurezza e l'alta direzione dell'Agenzia si è, infatti, rivelata una scelta vincente a favore di una rapidità di intervento non altrimenti realizzabile, parallelamente alla rapidità con cui si possono sviluppare le minacce nello spazio cibernetico.

Allo stesso modo, è stato opportunamente previsto un meccanismo di verifica parlamentare sull'attuazione, da parte dell'Agenzia, delle politiche di cybersicurezza, con particolare riferimento a quegli aspetti che impattano la sicurezza nazionale. Difatti, il Parlamento riceve, annualmente, dal Presidente del Consiglio, due relazioni "di rendicontazione", una delle quali al Comitato parlamentare per la sicurezza della Repubblica (COPASIR). Quest'ultimo Comitato, oltre ad avere la facoltà di chiedere l'audizione del Direttore generale dell'Agenzia su questioni di propria competenza, è destinatario di comunicazioni in ottemperanza a diversi obblighi informativi, stabiliti sia a livello normativo primario che secondario (ad esempio, circa le assunzioni, da parte dell'Agenzia, di personale a tempo determinato per lo svolgimento delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico, nonché dei contratti stipulati ai sensi del regolamento appalti in deroga).

Al di là delle costanti interazioni tra Agenzia e COPASIR, il Direttore generale dell'Agenzia è stato audito tre volte e il 30 giugno u.s. è stata trasmessa al Comitato la prima relazione sulle attività svolte a tutela della sicurezza nazionale nello spazio cibernetico.

[6] Così come previsto, rispettivamente, dall'articolo 11, comma 3, dall'articolo 6, comma 3 e dall'articolo 12, comma 8, del decreto-legge.
[7] Come previsto dall'articolo 2, comma 1, lettera b).
[8] In particolare, in relazione a quest'ultimo provvedimento, il CIC ha esercitato per la prima volta le funzioni che il decreto-legge 21 settembre 2019, n. 105, c.d. "decreto-legge perimetro" e i relativi provvedimenti attuativi attribuivano al Comitato interministeriale per la sicurezza della Repubblica - CISR – di cui alla legge 3 agosto 2007, n. 124 – fatta eccezione per quelle previste dall'articolo 5 del richiamato decreto-legge perimetro in materia di determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica.
[9] Come previsto dall'articolo 4, comma 2, lettera d).
[10] Come previsto dall'articolo 11, comma 4, del decreto-legge.

2. STRUTTURAZIONE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

Strutturazione dell'Agenzia per la Cybersicurezza Nazionale

Allo scopo di attuare le suddette autonomie, l'Agenzia ha profuso un elevato impegno nella elaborazione di provvedimenti normativi necessari a renderle effettive.

Si tratta, in primis, dei già citati quattro regolamenti, adottati con DPCM, che rappresentano il cardine del funzionamento dell'ente: 1) Regolamento di contabilità; 2) Regolamento di organizzazione e funzionamento; 3) Regolamento del personale; 4) Regolamento c.d. "appalti in deroga".

I primi 3 regolamenti, essenziali per concludere la fase di avvio della prima operatività dell'Agenzia, sono stati adottati in tempi assai brevi considerato che dopo soli 4 mesi dall'avvio dell'attività dell'Agenzia, avvenuto il 1° settembre 2021, sono stati adottati i DPCM. Lasso di tempo che, anche in assenza di detti provvedimenti, l'Agenzia ha, comunque, sin da subito, dedicato a svolgere le sue principali funzioni istituzionali, provvedendo alla immediata definizione di una strutturazione interna, ancorché provvisoria.

Il funzionamento e l'organizzazione interna dell'Agenzia sono, poi, ulteriormente disciplinati da circa 20 provvedimenti attuativi del Direttore generale dell'ACN.

Grazie al notevole impegno posto in essere dall'Agenzia e al costante supporto di Governo e Parlamento, a poco più di un anno dall'avvio della sua prima operatività, si è stati in grado di rendere giuridicamente e operativamente efficaci le suddette autonomie regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, come di seguito illustrato, secondo un approccio progressivamente incrementale.

ARCHITETTURA NAZIONALE: LIVELLI DI COORDINAMENTO

Attuazione della struttura organizzativa

Per quanto riguarda l'organizzazione dell'ente, l'articolo 6 del decreto-legge, nel rimandare al Regolamento la disciplina di dettaglio, ha previsto la possibilità di istituire fino ad un massimo di otto articolazioni di livello dirigenziale generale, nonché fino ad un massimo di trenta articolazioni di livello dirigenziale non generale. Il DPCM recante il Regolamento di organizzazione ha, quindi, previsto l'articolazione dell'Agenzia in sette uffici di livello dirigenziale generale, denominati *Servizi*, posti alle dipendenze del Direttore generale dell'Agenzia, confermando il numero massimo di trenta articolazioni di livello dirigenziale non generale.

> *La fissazione di tali limiti numerici a livello di norma primaria potrebbe non conciliarsi perfettamente con le esigenze di flessibilità della struttura. In tal senso, potrebbe essere ipotizzata una modifica della norma primaria volta a consentire maggiore flessibilità a parità di budget.*

I Servizi previsti dall'articolo 12 del DPCM 223/2021 sono:

- *Gabinetto;*
- *Autorità e sanzioni;*
- *Certificazione e vigilanza;*
- *Operazioni;*
- *Programmi industriali, tecnologici, di ricerca e formazione;*
- *Risorse umane e strumentali;*
- *Strategie e cooperazione.*

Gabinetto	Mantenimento quadro normativo nazionale cyber aggiornato Tavoli cyber interministeriali (CIC, NCS, Perimetro)
Autorità e sanzioni	Adempimento disposizioni decreti NIS, PSNC e Telco Sanzioni
Certificazione e vigilanza	Centro di Valutazione e Certificazione Nazionale (CVCN) Organismo di certificazione della sicurezza informatica (OCSI) Autorità nazionale di certificazione in materia di cybersicurezza Attività ispettiva e di verifica degli adempimenti di cybersicurezza
Operazioni	Computer Security Incident Response Team (CSIRT) Italia Monitoraggio, prevenzione, risposta ad attacchi cyber
Programmi industriali, tecnologici, di ricerca e formazione	Promozione programmi di investimento, industriali e di ricerca Centro nazionale di coordinamento in materia di cybersicurezza (NCC) Promozione formazione in cybersicurezza
Risorse umane e strumentali	Reclutamento, formazione e sviluppo professionale del personale Bilancio, procurement e logistica
Strategie e cooperazione	Predisposizione strategia nazionale di cybersecurity Elaborazione di policy nazionali e iniziative di awareness Relazioni internazionali e cooperazione

Tuttavia, in sede di prima applicazione, in relazione alle risorse umane disponibili, l'Agenzia ha provveduto ad attivare progressivamente solo i Servizi, le Divisioni e le articolazioni necessari per l'efficace svolgimento delle attività prioritarie. In particolare, al 30 settembre 2022, con successivi provvedimenti del Direttore generale, sono stati attivati i seguenti cinque Servizi:

- Gabinetto;
- Certificazione e vigilanza;
- Operazioni;
- Programmi industriali, tecnologici, di ricerca e formazione;
- Risorse umane e strumentali.

Le principali funzioni del Servizio Autorità e sanzioni e del Servizio Strategie e cooperazione sono, comunque, assicurate dalla suddivisione delle relative competenze tra i cinque Servizi già attivati.

Sono state, altresì, istituite sedici Divisioni, di cui nove di maggiore complessità, quali articolazioni di livello dirigenziale non generale, in relazione alla particolare delicatezza e rilevanza delle funzioni, che comportano notevoli responsabilità.

Il DPCM n. 223/2021 ha, inoltre, disciplinato nel dettaglio le funzioni del Direttore generale e del Vice Direttore generale.

Quale organo di vertice dell'Agenzia e, dunque, suo legale rappresentante, il Direttore generale ha la rappresentanza esterna, cura i rapporti esterni nazionali ed esteri, sottoscrive i contratti, ove non siano espressamente delegati i responsabili dei Servizi competenti, ovvero altro personale dell'Agenzia. Oltre alle suddette funzioni, attinenti alla sfera della rappresentanza esterna, il Direttore generale svolge i compiti previsti, a vario titolo, dalla normativa in materia di cybersicurezza nell'ambito degli organismi collegiali. In relazione, poi, all'esercizio delle sue competente in materia organizzativa e, in particolare, per l'adozione degli atti gestionali che impattano sulla struttura, sui processi organizzativi, sul funzionamento dell'Agenzia, per quelli di nomina, promozione, assegnazione, trasferimento ed incarichi del personale e per quelli strategici e di bilancio, nonché per l'esecuzione degli indirizzi degli organi di indirizzo politico, è stata prevista la partecipazione del Vice Direttore generale alle scelte di vertice.

Al Vice Direttore generale è attribuito il ruolo di coadiuvare il Direttore generale nella direzione dell'ente, sostituirlo nei casi di assenza o impedimento e, sulla base di apposito provvedimento del Direttore generale, può esercitare tutte le specifiche funzioni attribuitegli o delegategli, nonché sovrintendere e coordinare i Servizi e le altre articolazioni dell'Agenzia. Inoltre, il Vice Direttore generale partecipa a tutti i consessi decisionali, consultivi e di condivisione informativa dell'Agenzia.

Al 30 settembre 2022, in ragione della fase di *start-up*, non sono state istituite né sedi secondarie, né unità distaccate presso enti e istituzioni dell'Unione europea o presso Ambasciate e

Rappresentanze italiane operanti presso organi dell'UE o Organizzazioni internazionali. La decisione circa l'istituzione di sedi secondarie o distaccate spetta, ai sensi dell'articolo 15 del DPCM n. 223/2021, al Comitato di Vertice, su proposta del Direttore generale.

Attuazione dell'autonomia patrimoniale, contabile e finanziaria

Per quanto riguarda l'autonomia patrimoniale, contabile e finanziaria, sempre l'articolo 6 del decreto-legge indica quali organi dell'Agenzia, oltre al Direttore generale, anche il Collegio dei revisori dei conti, le cui funzioni sono sempre disciplinate dal Regolamento di organizzazione e funzionamento.

In particolare, per quest'ultimo è stato previsto che sia composto da un magistrato della Corte dei conti, in servizio o in quiescenza, che lo presiede, da un componente effettivo, designato dal Ministero dell'economia e delle finanze e da un ulteriore componente effettivo e un componente supplente, scelti entrambi tra soggetti, in servizio o in quiescenza appartenenti ai ruoli della magistratura amministrativa, contabile o dell'Avvocatura dello Stato, ovvero tra professori universitari ordinari di contabilità pubblica o discipline similari, ovvero tra alti dirigenti dello Stato.

Il presidente e i componenti del Collegio sono stati nominati con provvedimento del Direttore generale dell'Agenzia del 14 giugno 2022, su deliberazione del Comitato di Vertice, che, come già rappresentato, si è all'uopo riunito il 14 giugno 2022, sotto la presidenza dell'Autorità delegata. È stato, inoltre, adottato il decreto del Presidente del Consiglio dei ministri che stabilisce il relativo compenso, così come previsto dall'articolo 7 del DPCM n. 223/2021.

Il Collegio dei revisori dei conti ha, pertanto, avviato le sue attività volte a effettuare, tra l'altro, il riscontro degli atti della gestione finanziaria, svolgere verifiche di cassa e di bilancio, esprimere parere sul progetto di bilancio preventivo, nonché sul rendiconto annuale.

Il 28 luglio u.s., con decreto del Presidente del Consiglio dei ministri, è stato poi approvato il primo bilancio previsionale dell'Agenzia (a seguito dell'esame sia da parte del CIC che del Ministero dell'economia e delle finanze) che, a causa delle difficoltà connesse alla fase di prima organizzazione, è stato adottato con provvedimento del Direttore generale del 24 giugno 2022, su parere del Collegio dei revisori dei conti.

Attuazione del sistema di gestione del personale

Per quanto riguarda la dotazione organica necessaria al funzionamento dell'Agenzia, giova richiamare che il decreto-legge rimette ad un apposito regolamento la definizione della disciplina applicabile al contingente di personale addetto all'ACN, anche in deroga alle vigenti disposizioni

di legge, nel rispetto dei principi generali dell'ordinamento giuridico tenuto conto delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia. In attuazione di tale norma, è stato adottato il già menzionato DPCM n. 224/2021.

A tal riguardo, è necessario precisare che, in ragione dell'equiparazione operata dall'articolo 12 del decreto-legge tra il trattamento economico del personale della Banca d'Italia e quello dell'ACN, specie tenuto conto delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico, è stato adottato un sistema del personale analogo a quello adottato dalla Banca, sia da un punto di vista normativo, sia organizzativo, pur con i dovuti adeguamenti alle peculiari prerogative attribuite all'ACN.

Il regolamento ha, dunque, previsto che il ruolo del personale dell'Agenzia sia distinto in due diverse aree: "Area manageriale ed alte professionalità" ed "Area operativa". Nell'Area manageriale e alte professionalità viene inquadrato il personale afferente ai segmenti professionali di: Direttore centrale; Direttore (rispettivamente equiparabili a dirigenti di livello generale e non); Consigliere ed Esperto. Viceversa, nell'Area operativa sono previsti i segmenti professionali di Coordinatore ed Assistente.

Nel disciplinare il trattamento del personale, il regolamento delinea il sistema di assunzione, feedback, valutazione delle performance, progressione in carriera e formazione e sviluppo del personale, nonché altri istituti classici del rapporto di lavoro quali l'orario di lavoro, il trattamento economico, i congedi, le assenze, le sanzioni disciplinari, i casi di cessazione dal servizio e gli obblighi del dipendente. Sono state, inoltre, definite le procedure per il reinquadramento nei ruoli dell'Agenzia del personale proveniente dal Dipartimento delle informazioni per la sicurezza e dalle altre amministrazioni, messo a disposizione ai sensi di cui all'articolo 17, comma 8, del decreto-legge.

Il decreto-legge prevede, inoltre, la possibilità di procedere anche ad assunzioni a tempo determinato di soggetti in possesso di alta e particolare specializzazione, individuati attraverso adeguate modalità selettive[11].

Tuttavia, la norma non si è rivelata del tutto persuasiva per favorire e incentivare l'acquisizione di tali figure specializzate – particolarmente necessarie per le funzioni di tutela della sicurezza nazionale – in particolare per la breve durata degli stessi che rappresentava un disincentivo soprattutto per quelle figure professionali collocate all'estero. Pertanto, al fine di perfezionare la previsione normativa, è stata introdotta, con il decreto-legge 21 marzo 2022, n. 21, recante "*Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina*" (c.d. decreto-legge Ucraina), una disciplina *ad hoc* per i contratti a tempo determinato stipulati per lo svolgimento delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia

[11] Articolo 12, comma 2, lettera b), del decreto-legge.

(introducendo il comma 8-bis all'articolo 12). L'articolo 29, comma 6, del citato decreto-legge Ucraina ha, infatti, previsto che i predetti contratti possano avere una durata massima di quattro anni, rinnovabile per periodi non superiori ad ulteriori complessivi quattro anni. La durata complessiva superiore, fino ad otto anni, dovrebbe riuscire ad assicurare la copertura con personale altamente specializzato delle progettualità relative alla tutela della sicurezza nazionale per l'intera durata delle stesse, anche incentivando il rientro di tali figure professionali dall'estero.

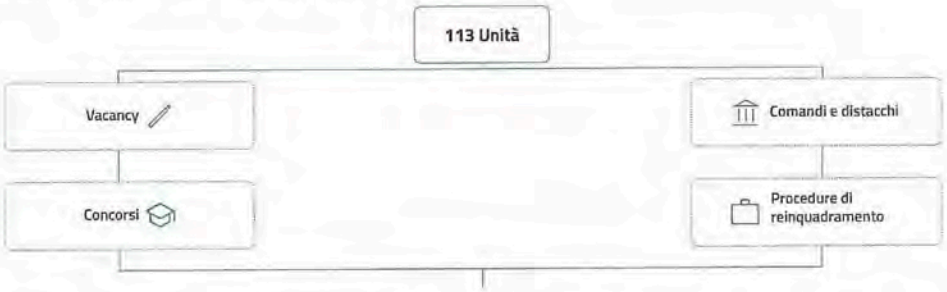
In considerazione della specificità di tale, ultima disciplina, la medesima disposizione prevede che di tali assunzioni sia fatta comunicazione al COPASIR nell'ambito della relazione annuale di cui all'articolo 14, comma 2, del decreto-legge.

In relazione alla dotazione organica, al 30 settembre l'Agenzia impiega 113 unità di personale (a fronte delle 300 previste dalla dotazione organica per il 2023)[12].

Tali risorse sono state acquisite attraverso la definizione e l'implementazione di tutti gli strumenti funzionali all'acquisizione di risorse umane attivabili dall'Agenzia; specificamente:

- le speciali procedure di inquadramento previste dall'articolo 17, comma 8, del decreto-legge, che hanno permesso di assumere nel ruolo dell'ACN il personale messo a disposizione da altre Amministrazioni per garantire la prima operatività dell'ACN, concluse il 30 giugno u.s.;
- sei procedure concorsuali, bandite il 22 febbraio 2022 e concluse nel mese di luglio scorso;
- undici procedure di selezione per l'assunzione a tempo determinato con contratti di diritto privato ("*vacancy*") di persone in possesso di alta e particolare specializzazione per lo svolgimento di attività assolutamente necessarie all'operatività dell'Agenzia ovvero per la realizzazione di specifiche progettualità;
- messa a disposizione dell'Agenzia di personale proveniente da altre Amministrazioni pubbliche tramite distacchi, comandi, fuori ruolo o altre analoghe posizioni previste dagli ordinamenti di appartenenza.

CANALI DI INGRESSO - 30 SETTEMBRE 2022



[12] Entro la fine dell'anno, la compagine del personale di ruolo a tempo indeterminato dell'Agenzia si dovrebbe attestare sulle circa 140 unità.

3. L'ATTUAZIONE DELLE FUNZIONI DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

L'attuazione delle funzioni dell'Agenzia per la Cybersicurezza Nazionale

Ai sensi dell'articolo 7 del decreto-legge, l'Agenzia è riconosciuta quale Autorità nazionale per la cybersicurezza. In correlazione a tale ruolo centrale, l'ACN ha, dunque, il compito di assicurare il coordinamento tra i soggetti pubblici coinvolti in questioni di cybersicurezza a livello nazionale e di promuovere la realizzazione di azioni comuni volte ad assicurare la sicurezza e resilienza cibernetiche in funzione dello sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni. Ciò anche in vista del conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore.

Tale ruolo di coordinamento, nonché di promozione di azioni comuni, è svolto dall'Agenzia sia in seno ai diversi consessi istituzionali che essa presiede, tra cui il Nucleo per la cybersicurezza e il Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica (dei quali si dirà più nel dettaglio nel prosieguo), sia attraverso il coinvolgimento e la collaborazione con altre istituzioni, con il mondo dell'accademia e con il settore privato nelle progettualità che essa dirige o supporta, ad esempio quelle legate all'investimento 1.5 "*Cybersecurity*" del PNRR, di cui l'ACN è soggetto attuatore.

In particolare, tale collaborazione dell'ACN con il settore privato si concretizza anche in un ruolo di sensibilizzazione e "accompagnamento" delle aziende verso l'efficace applicazione della normativa settoriale cyber e dei relativi obblighi e misure.

A titolo di premessa all'illustrazione, nello specifico, delle attività poste in essere per l'attuazione delle funzioni stabilite dalla normativa cyber, è necessario specificare che alcune competenze esercitate dall'Agenzia sono attribuite *ex novo* dal decreto-legge, mentre altre ad esito del trasferimento dalle istituzioni che le esercitavano ai sensi della precedente architettura nazionale cyber. Pertanto, l'attuazione – nelle modalità che verranno descritte – delle suddette funzioni ha comportato, da un lato, la progettazione e lo sviluppo, ab origine, delle più idonee modalità di implementazione di quelle di nuova creazione, dall'altro, la definizione e adozione dei DPCM, e dei relativi Protocolli attuativi, volti a disciplinare il passaggio delle funzioni (come disposto dall'articolo 17, comma 5, del decreto-legge).

Quest'ultimo processo ha interessato, in particolare, il passaggio dal Dipartimento delle informazioni per la sicurezza, dal Ministero dello sviluppo economico (MiSE), dalla Presidenza del Consiglio dei ministri (in particolare il Dipartimento per la transizione digitale) e dall'Agenzia per l'Italia digitale (AgID).

Al 30 settembre, sono stati adottati tutti i DPCM di trasferimento dalle suddette Amministrazioni (e relativi n. 6 Protocolli d'intesa), in particolare: il 16 settembre, è stato adottato il DPCM di trasferimento delle funzioni, dei beni strumentali e della documentazione dal DIS; il 15 giugno 2022, è stato adottato il DPCM di trasferimento dal MiSE; il 1° settembre 2022 è stato adottato il DPCM di trasferimento dal MiTD e da AgID.

La finalizzazione in tempi brevi dei sopra menzionati DPCM è stata frutto di un rilevante impegno sia da parte dell'ACN che dalle Amministrazioni trasferenti, volto ad individuare non solo le funzioni oggetto di trasferimento, ma anche i relativi beni strumentali e documentali funzionali al loro svolgimento. Ciò è valso, in particolare, per il trasferimento delle funzioni dal MiSE, che rappresentava un necessario presupposto per l'attivazione del CVCN da effettuarsi, secondo i termini sanciti dal decreto-legge perimetro, entro il 30 giugno 2022.

Delle modalità di attuazione, da parte dell'ACN, delle specifiche funzioni trasferite si darà conto, unitamente alle funzioni attribuite *ex novo,* nelle seguenti sezioni tematiche.

Strategia nazionale di cybersicurezza

Una delle attività preminenti portate avanti nei primi mesi di operatività, è stata l'elaborazione della Strategia nazionale di cybersicurezza, adottata – come detto – con DPCM del 17 maggio 2022, la cui predisposizione è stata curata, ai sensi dell'articolo 7, comma 1, lettera b), dall'ACN. La strategia individua tre obiettivi fondamentali – protezione, risposta e sviluppo – e relative misure, funzionali ad assicurare la concreta attuazione della Strategia dal punto di vista organizzativo, di policy e prettamente operativo. Per poter realizzare fattivamente gli obiettivi descritti, la Strategia attribuisce, inoltre, grande rilevanza a una serie di fattori abilitanti: formazione; promozione della cultura della sicurezza cibernetica; cooperazione. Particolare importanza assume il ricorso alla Partnership Pubblico-Privato, che permea l'intero documento.

In particolare, le 82 misure da attuare, individuate, nello specifico, nel correlato Piano di implementazione, sono state suddivise in aree tematiche, per ognuna delle quali sono stati individuati gli attori responsabili per l'attuazione e gli altri soggetti a vario titolo interessati. Pertanto, considerata la complessità del documento, al fine di garantire la piena e pronta attuazione della Strategia, è stata avviata un'importante attività di coordinamento, con la costituzione di diversi tavoli di lavoro cui partecipano, coordinate dall'Agenzia, le amministrazioni individuate quali responsabili o co-responsabili di una o più misure. Ciò allo scopo di stabilire, entro dodici mesi dall'adozione della Strategia, le metriche e *key performance indicator*-KPI di cui alla misura #82 del Piano. In particolare, i suddetti KPI, sulla base di appositi indicatori, consentiranno di misurare quantitativamente lo stato di attuazione di ogni singola misura e, a partire dal secondo anno (ovvero da gennaio 2023), esprimere una valutazione retrospettiva sulla performance relativa all'implementazione della specifica misura. Il 12 luglio 2022 si è tenuta la prima riunione di coordinamento, presieduta dall'Agenzia, con tutte le amministrazioni coinvolte, cui hanno fatto seguito ulteriori incontri con gruppi di soggetti pubblici divisi per cluster di misure, al fine di iniziare a definire metriche e indicatori.

> *A tal riguardo, al fine di supportare le attività delle Amministrazioni pubbliche volte a rendere il Paese più resiliente e sicuro nel dominio cibernetico, sarebbe auspicabile prevedere nella legge di bilancio, per il finanziamento delle misure previste nella Strategia nazionale di cybersicurezza, la creazione nello stato di previsione del MEF di un fondo per l'attuazione della Strategia di cybersicurezza e di un fondo per la gestione della cybersicurezza, adeguatamente dimensionati.*

Funzioni ai sensi della normativa NIS (d. lgs. n. 65/2018)

Tra le principali innovazioni sulle quali si basa la riformata architettura di cybersicurezza, l'articolo 7, comma 1, lettera d), a tutela dell'unità giuridica dell'ordinamento, attribuisce all'Agenzia per la cybersicurezza nazionale il ruolo di **Autorità nazionale competente e punto di contatto unico** in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo 18 maggio 2018, n. 65 ("decreto legislativo NIS"), che recepisce nell'ordinamento interno la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante *Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione.*

Tali funzioni, infatti, prima dell'entrata in vigore del decreto-legge, erano attribuite ad un'ampia pluralità di amministrazioni, nonché, relativamente alla materia dell'assistenza sanitaria e alla distribuzione di acqua potabile, anche alle Regioni e alle Province autonome di Trento e Bolzano. A fronte di oltre venti differenti Autorità competenti NIS, vi era, poi, il Dipartimento delle informa-

zioni per la sicurezza che fungeva, nella previgente architettura, da punto di contatto unico.

Con il decreto-legge, l'Agenzia è quindi diventata Autorità nazionale competente per la sicurezza delle reti e dei sistemi informativi, assicurando un'unicità di approccio a livello nazionale per le misure di sicurezza e accentrando, così, anche le funzioni di accertamento delle violazioni e l'irrogazione delle sanzioni previste nel citato decreto legislativo NIS. Al contempo, considerato l'importante patrimonio conoscitivo, nei settori di rispettiva competenza, delle precedenti Autorità competenti NIS – che risulta fondamentale per assicurare una completa identificazione degli operatori dei servizi essenziali (OSE) – le stesse sono divenute "autorità di settore", con il compito di proporre all'autorità nazionale competente NIS-ACN le variazioni all'elenco degli OSE, secondo criteri stabiliti dallo stesso decreto legislativo NIS.

L'attuazione della suddetta riforma normativa è subordinata all'adozione di uno o più DPCM, con cui viene regolamentato il passaggio di funzioni tra le amministrazioni interessate. Considerato, come sopra anticipato, che tali amministrazioni sono 27, si tratta di attività attuativa particolarmente gravosa.

Il suddetto passaggio di consegne è già stato realizzato con riferimento al Ministero dello sviluppo economico. Infatti, con il citato DPCM del 15 giugno 2022, è stato trasferito l'elenco degli OSE e le funzioni di autorità di regolamentazione, ispezione e vigilanza per il settore infrastrutture digitali, sotto-settori IXP, DNS, TLD, nonché per i servizi digitali. Per i restanti settori, che comprendono sia Amministrazioni centrali che Regioni, i lavori per i trasferimenti di funzioni sono in corso di finalizzazione.

Allo stesso modo, con il menzionato DPCM del 16 settembre 2021, è stato operato il trasferimento di funzioni dal DIS all'Agenzia, rendendo efficace, dunque, la designazione dell'Agenzia come punto di contatto unico ai fini del decreto legislativo NIS e la conseguente partecipazione dell'ACN ai relativi consessi internazionali, tra cui il *NIS Cooperation Group* e il *CSIRT Network* (tali gruppi, stabiliti a livello europeo, rappresentano dei consessi di raccordo, rispettivamente, dei Punti di contatto – livello policy – e dei CSIRT – livello tecnico – di ciascuno Stato membro).

Grazie al trasferimento operato con il DPCM da ultimo citato, è stata, inoltre, garantita, senza soluzione di continuità, l'operatività del CSIRT Italia, oggetto di specifico approfondimento nella sezione dedicata alle funzioni di preparazione, prevenzione, gestione e risposta a eventi cibernetici.

Funzioni di certificazione della cybersicurezza Cybersicurezza Nazionale

Sempre in estrinsecazione del ruolo di Autorità nazionale di cybersicurezza, l'Agenzia è anche Autorità nazionale di certificazione della cybersicurezza.

Ciò si concretizza, dunque, ai sensi dell'articolo 7, comma 1, lettera e), nell'accentramento in capo all'Agenzia del potere di rilasciare le certificazioni in materia ai sensi delle diverse normative vigenti. L'Agenzia è, infatti, Autorità nazionale di certificazione della cibersicurezza ai sensi dell'articolo 58 del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019 (d'ora innanzi *Cybersecurity Act*) e inoltre incorpora, a seguito del trasferimento dal MiSE, l'Organismo di certificazione della sicurezza informatica (OCSI) – il quale certifica , ai sensi del DPCM del 30 ottobre 2003, prodotti commerciali secondo uno schema di certificazione nazionale, internazionalmente riconosciuto da Paesi che aderiscono, insieme all'Italia, ad accordi di mutuo riconoscimento – e il Centro di valutazione e certificazione nazionale (CVCN), istituito ai sensi del decreto-legge perimetro. Tali funzioni – compresa la prima operatività del CVCN, in conformità al termine del 30 giugno 2022 stabilito dall'articolo 16, comma 9, decreto-legge – sono state avviate dall'Agenzia anche grazie alla menzionata acquisizione di beni strumentali e risorse umane dal MiSE , nonché alle recenti assunzioni di personale tecnico ad esito delle citate procedure concorsuali.

In tale ambito, l'Agenzia avrà il potere di emettere, tramite OCSI, certificati europei di livello "elevato", dal momento in cui i sistemi di certificazione europei in corso di elaborazione (in particolare, *cloud* e 5G) saranno adottati a livello comunitario.

L'Agenzia, quale Autorità nazionale di certificazione, ha fornito un ampio contributo alla redazione del decreto legislativo 3 agosto 2022, n. 123, recante norme di adeguamento della normativa nazionale alle disposizioni del Titolo III «*Quadro di certificazione della cibersicurezza*» del *Cybersecurity Act*.

Attuazione del Perimetro di Sicurezza Nazionale Cibernetica (PSNC)

Nella rinnovata architettura istituzionale, l'Agenzia ha assunto un ruolo centrale anche per l'attuazione del Perimetro di sicurezza nazionale cibernetica, in quanto ha accentrato le funzioni regolamentari, di certificazione, ispezione, vigilanza e sanzionatorie, precedentemente attribuite al DIS, al MiSE e alla PCM.

Infatti, l'ACN, avendo acquisito le funzioni previamente esercitate dal DIS, supporta il Presidente del Consiglio nel coordinamento della coerente attuazione delle disposizioni PSNC. Alla luce di

ciò, l'Agenzia svolge una funzione di raccordo inter-istituzionale tra le amministrazioni interessate che si concretizza, ad esempio, attraverso l'avvenuto trasferimento del Tavolo per l'attuazione del perimetro di sicurezza nazionale cibernetica presso l'ACN, che lo presiede. A tal riguardo, l'Agenzia ha già provveduto ad attivare il consesso inter-istituzionale a seguito del suo trasferimento, che si è riunito il 25 marzo u.s. per esprimersi sul testo del DPCM 18 maggio 2022, n. 92, recante *Regolamento in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa*, ai sensi dell'articolo 1, comma 7, lettera b), del decreto-legge perimetro.

Tale DPCM, che costituisce l'ultimo dei provvedimenti di attuazione previsti dal decreto-legge perimetro, contiene le procedure, le modalità ed i termini da seguire per l'accreditamento dei Centri di valutazione (CV) e dei Laboratori di prova (LAP), e per la gestione dei raccordi del CVCN con i LAP e i CV, norme queste che supporteranno il CVCN nella valutazione delle condizioni di sicurezza e dell'assenza di vulnerabilità note in relazione ai prodotti ICT appartenenti a specifiche categorie e destinati ad essere impiegati nei beni ICT dei soggetti perimetro per l'esercizio di funzioni/servizi essenziali per la sicurezza nazionale. L'Agenzia ha dedicato notevole impegno per la finalizzazione del testo, al fine di completare, prima dell'avvio delle attività del CVCN, l'adozione della normativa secondaria di attuazione del PSNC.

In attuazione del suddetto DPCM, l'Agenzia ha adottato, con provvedimento del Direttore generale del 11 agosto u.s., le determinazioni tecniche per l'accreditamento dei LAP. In particolare, in tale provvedimento sono indicati degli specifici obblighi posti in capo ai LAP, sia in relazione all'accreditamento che alla successiva operatività. Si tratta, ad esempio, di requisiti tecnici, logistici, di competenza ed esperienza, di misure di sicurezza informatica, nonché di particolari requisiti per l'espletamento di alcune attività come, ad esempio, il divieto di divulgazione ovvero la notifica entro le 24 ore delle limitazioni di operatività dei LAP superiori alle 24 ore. Le determinazioni tecniche contengono anche la definizione della prima area di accreditamento, che consentirà ai laboratori di eseguire test di sicurezza, su mandato del CVCN, su componenti software e apparati di rete.

L'Agenzia ha, inoltre, dato immediata esecuzione ai compiti presi dal DIS in materia di PSNC, sia con riferimento alle notifiche di incidente ricevute dal CSIRT Italia, sia in riferimento agli altri adempimenti previsti per i soggetti perimetro, fornendo a quest'ultimi un supporto collaborativo, volto ad ottenere l'adeguata attuazione degli obblighi.

Attuazione delle funzioni relative alla normativa in materia di "poteri speciali"

L'articolo 7, comma 1, lettera g), prevede che l'Agenzia, per gli specifici ambiti di competenza, partecipi anche al Gruppo di coordinamento per l'esercizio dei poteri speciali (c.d. *Golden Power*) di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56. Al riguardo, con il c.d. decreto-legge Ucraina sono state apportate importanti modifiche alla richiamata normativa, ridefinendo, nello specifico, i poteri speciali in materia di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G e cloud, nonché rafforzando la disciplina *cyber*. Gli articoli 28 e 29 del citato decreto-legge, sui quali l'Agenzia ha espresso specifico parere, attribuiscono all'ACN specifiche funzioni in materia, ad esempio coinvolgendola nel processo di individuazione di servizi, beni, rapporti, attività e tecnologie rilevanti ai fini della sicurezza cibernetica ulteriori ai servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G e nell'esecuzione, tramite il CVCN, delle precipue verifiche di sicurezza. In particolare, viene stabilita la presenza di rappresentanti dell'ACN nella composizione del citato Gruppo di coordinamento per l'esercizio dei poteri speciali e del relativo Comitato di monitoraggio, specificando che, per l'espressione delle valutazioni tecniche e per l'esecuzione delle conseguenti attività di monitoraggio, questi ultimi si avvalgono anche del CVCN. In questo senso, fin dalla sua istituzione, l'ACN ha contribuito all'assolvimento di tali attività, partecipando alle sedute del Gruppo di coordinamento e del Comitato di monitoraggio, fornendo i pareri di competenza.

Attuazione delle funzioni relative al Codice dell'amministrazione digitale e al Cloud nazionale

Ai sensi dell'articolo 7, lettera *m)*, l'Agenzia per la cybersicurezza nazionale assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti che includono, tra le altre, l'adozione di linee guida individuanti soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture, nonché regole tecniche di cybersicurezza per l'attuazione del Codice dell'Amministrazione Digitale-CAD di cui al decreto legislativo 7 marzo 2005, n. 82, come successivamente modificato e integrato dal decreto legislativo 22 agosto 2016, n. 179 e dal decreto legislativo 13 dicembre 2017, n. 217. Spetta all'Agenzia, inoltre, stabilire i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle

infrastrutture digitali per la pubblica amministrazione, inclusa l'infrastruttura *cloud* nazionale.
Per quanto riguarda le linee guida, l'Agenzia ha contribuito, anche prima dell'effettivo trasferimento della funzione, alla definizione delle stesse, fornendo parere all'Agenzia per l'Italia digitale in merito al contenuto della determina n. 628/2021 concernente il Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi *cloud* per la pubblica amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi *cloud* per la pubblica amministrazione.
Allo stesso modo, in relazione al *cloud* nazionale, l'Agenzia ha collaborato a stretto contatto con il Dipartimento per la trasformazione digitale per l'elaborazione della Strategia nazionale del *cloud* per la PA di settembre 2021. In attuazione di tale Strategia, l'ACN ha adottato, con due determine del Direttore generale, il modello per la predisposizione dell'elenco e della classificazione di dati e di servizi e le ulteriori caratteristiche dei servizi *cloud* e requisiti per la qualificazione.
L'attuazione della Strategia richiede, ai fini della strutturazione e migrazione dei dati nel cloud nazionale, un procedimento di classificazione dei dati delle Pubbliche Amministrazioni. Ai fini dell'attuazione di tale processo, l'ACN ha avviato i processi e predisposto gli strumenti funzionali alla realizzazione del *cloud* nazionale. Ad esempio, per quanto riguarda le attività di classificazione dei dati delle Amministrazioni locali, sono state evase le pratiche di circa 16.000 amministrazioni tramite la piattaforma web padigitale2026; per la classificazione dei dati delle Amministrazioni centrali, ad esito di una collaborazione con SOGEI, è stato elaborato un apposito algoritmo di classificazione dei servizi.

Attuazione delle funzioni per la sicurezza delle comunicazioni elettroniche

Nella rinnovata architettura istituzionale cyber e a seguito della recente novella del Codice delle comunicazioni elettroniche (decreto legislativo 8 novembre 2021, n. 207, che ha modificato il decreto legislativo n. 259/2003, alla cui predisposizione l'Agenzia ha fornito il suo contributo), l'ACN ha acquisito le funzioni previamente esercitate dal Ministero dello sviluppo economico in materia di sicurezza delle comunicazioni elettroniche. Nello specifico, l'Agenzia è competente per la definizione delle misure di sicurezza (tecniche e organizzative) per reti pubbliche e servizi di comunicazione elettronica accessibili al pubblico, delle soglie di significatività degli incidenti, nonché per la ricezione delle notifiche di incidenti e lo svolgimento delle ispezioni.

Attuazione della funzione di preparazione, prevenzione, gestione e risposta a eventi cibernetici

Con riferimento alle funzioni di cui all'articolo 7, comma 1, lettera n), ha fin da subito posto in essere e sviluppato le prescritte attività di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici. Ciò anche grazie al tempestivo trasferimento, con il DPCM del 16 settembre 2021, del CSIRT Italia dal Dipartimento delle informazioni per la sicurezza e alla sua immediata messa in esercizio.
L'Agenzia ha assicurato, inoltre, anche attività a supporto di soggetti colpiti da attacchi cyber al fine di sostenerli, in particolare, nelle azioni di contenimento e *remediation*.
In tale ambito, fin dall'avvio dell'operatività dell'ACN, sono state stabilite idonee forme di collaborazione e sinergia con la Polizia postale e delle comunicazioni, per assicurare il pieno coordinamento tra attività di resilienza ed attività investigative.

> *Al contempo, al fine di assicurare che le attività del personale dell'ACN vengano svolte nel modo più efficace, sarebbe auspicabile ipotizzare un intervento normativo volto ad accrescere la tutela giuridica per il personale dell'Agenzia che va ad agire sui beni ICT che sono stati soggetti ad un attacco cyber.*

L'attività di analisi è sempre posta, inoltre, a beneficio delle Amministrazioni facenti parte del Nucleo per la cybersicurezza (di cui si dirà più nel dettaglio nel prosieguo) con le quali sono state prontamente condivise nuove o emergenti vulnerabilità tecniche, *early warning* e bollettini, nonché sono stati analizzati i principali eventi cibernetici , fornendo approfondimenti circa le metodologie di attacco riscontrate, i *threat actor* coinvolti, le misure raccomandate e le lezioni apprese.
Nell'ambito della preparazione agli eventi cyber rientra anche la partecipazione alle esercitazioni nazionali e internazionali, di cui all'articolo 7, comma 1, lettera o), che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese; l'ACN vi ha dato attuazione già dal primo mese di attività, assicurando la partecipazione a livello nazionale e internazionale (specie UE, NATO, multilaterali).

Mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza

Con l'articolo 7, comma 1, lettera p), viene attribuita all'Agenzia la funzione di curare e promuovere la definizione e il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza.

In tale specifico ambito, sin dalla prima operatività dell'Agenzia, sono state poste in essere molteplici ed eterogenee attività volte al raggiungimento delle finalità previste dalla lettera p) in argomento che hanno riguardato, in particolare, l'espressione di pareri di competenza sulle iniziative legislative del Governo e del Parlamento, la predisposizione di contributi di risposta ad atti di sindacato ispettivo, la redazione di convenzioni e accordi stipulati dall'Agenzia.

Questa funzione è stata attuata, dunque, dall'Agenzia attraverso la predisposizione dei già citati DPCM di passaggio delle funzioni e di funzionamento dell'ACN, l'espressione dei pareri sui sopra individuati atti legislativi, nonché tramite l'adozione di atti "propri" di regolamentazione come, ad esempio, la circolare del Direttore generale dell'ACN del 21 aprile 2022 che, in attuazione dell'articolo 29 del citato decreto-legge Ucraina, individua le categorie per le quali è suggerita la diversificazione delle soluzioni tecnologiche, nonché relative raccomandazioni procedurali.

Ulteriormente, al fine di incrementare la capacità di allerta e la possibilità di venire a conoscenza di eventi cyber a danno di soggetti nazionali migliorando, così, anche l'attività di monitoraggio, rilevamento gestione e risposta a incidenti cibernetici, l'Agenzia ha fornito il proprio contributo alla modifica normativa (adottata con l'art. 37-*quater* del decreto-legge 9 agosto 2022, n. 115, convertito, con modificazioni, dalla legge 21 settembre 2022, n. 142) del citato decreto-legge perimetro, volta ad introdurre l'obbligo di notifica, entro 72 ore, da parte dei soggetti perimetro circa gli incidenti impattanti qualsiasi bene ICT del soggetto inserito nel PSNC e non solo i beni ICT inseriti nel perimetro.

Sempre nell'ambito della normativa concernente il PSNC, con il fine di migliorarne l'operatività, l'Agenzia ha contribuito alla modifica dell'articolo 5 del d.l. n. 105/2019, in materia di determinazioni del Presidente del Consiglio dei ministri, assunte su deliberazione del Comitato interministeriale per la sicurezza della Repubblica. Infatti, è stato previsto che, laddove necessario, i provvedimenti adottati in relazione alla disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati possano andare anche in deroga alle vigenti disposizioni, nel rispetto dei princìpi generali dell'ordinamento giuridico, dovendo fornire, al contempo, indicazione delle principali norme a cui si intende derogare, con specifica motivazione. È quindi previsto che tali provvedimenti presidenziali, anche in ragione dell'urgenza di tutelare la sicurezza nazionale, non siano soggetti al controllo preventivo di legittimità di cui all'articolo 3 della legge 14 gennaio 1994, n. 20.

Relazioni e cooperazione internazionale

L'attività di cooperazione internazionale nella materia della cybersicurezza, ai sensi dell'articolo 7, comma 1, lettera q), è coordinata dall'Agenzia in raccordo con il Ministero degli affari esteri e della cooperazione internazionale-MAECI. Allo scopo di assicurare nel miglior modo il predetto coordinamento, nonché un efficace posizionamento internazionale dell'Agenzia e sviluppo di una strutturata rete di relazioni diplomatiche, presso quest'ultima è stato distaccato del personale diplomatico di quel Ministero.

Per quanto riguarda le funzioni di cui alle lettere q), s) e t) del più volte citato articolo 7, concernenti le attività di rilievo internazionale dell'Agenzia (sia dal punto di vista del coordinamento della cooperazione internazionale che della stipula di accordi con istituzioni, enti e organismi di altri Paesi), l'Agenzia ha, fin da subito, avviato un processo di accreditamento con gli omologhi esteri e di definizione, sviluppo e rafforzamento della propria postura internazionale, partecipando ai fora internazionali ed europei, in ambito NATO, Unione europea e OSCE, cui a vario titolo partecipa l'Italia, nei quali vengono discusse e definite le politiche e le norme in materia cyber.

Si tratta, in particolare, dell'*Horizontal Working Party on Cyber Issues* (HWPCI) presso il Consiglio dell'Unione europea, dello *European Cybersecurity Certification Group* (ECCG), dell'*Informal Working Group* in ambito cyber presso l'OSCE, nonché della Rete di CSIRT. A livello bilaterale, sono state avviate e mantenute diverse interlocuzioni e rapporti di collaborazione con le omologhe agenzie, autorità ed enti stranieri, tra cui, a titolo esemplificativo, l'Agenzia francese di cybersicurezza-ANSSI, l'Autorità tedesca di cybersicurezza-BSI, il Centro belga per la cybersicurezza-CCB, l'Agenzia statunitense CISA e l'Israel National Cyber Directorate.

L'Agenzia ha, inoltre, espresso i rappresentanti nazionali presso il *Management Board della European Union Agency for Cybersecurity* (ENISA) e i relativi *National Liasons Officer*, nonché i rappresentanti italiani presso il *European Cybersecurity Competence Center* (ECCC).

Questi ultimi sono stati nominati il 28 febbraio 2022, con decreto del Presidente del Consiglio dei ministri, in attuazione della lettera aa) del medesimo articolo 7, comma 1, che stabilisce anche la designazione dell'Agenzia quale Centro nazionale di coordinamento (NCC) ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il ECCC e la rete dei centri nazionali di coordinamento.

Sviluppo di competenze e capacità industriali, tecnologiche e scientifiche

Ai sensi dell'articolo 7, comma 1, lettera r), l'Agenzia svolge funzioni in merito allo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore.

In attuazione delle suddette funzioni, sono state avviate attività su più fronti, tra cui: collaborazioni con il mondo dell'università e della ricerca, nonché con il sistema produttivo nazionale e con le principali realtà nazionali (*venture capital*, SGR, fondi di investimento, etc.), che promuovono e sostengono a diverso titolo programmi di accelerazione e/o incubazione di *startup* per innovazione tecnologica in ambito *cybersecurity*; progettualità, nell'ambito della *Mission 1, Componente 1, Investimento 1.5: Cybersecurity* del PNRR, di cui l'Agenzia è soggetto attuatore; attivazione del Comitato-tecnico scientifico istituito presso l'Agenzia.
Per quanto riguarda le collaborazioni con il mondo dell'università e della ricerca, sono state sottoscritte circa 5 convenzioni.

Per quanto riguarda il PNRR, una delle principali linee strategiche che l'Agenzia ha seguito riguarda il potenziamento della resilienza cyber della Pubblica Amministrazione per la messa in sicurezza dei dati e dei servizi dei cittadini. A tal fine, sono stati realizzati 4 Avvisi Pubblici volti all'identificazione e alla selezione di Pubbliche Amministrazioni, centrali e locali, che possano agire in qualità di Soggetti realizzatori di interventi di potenziamento della resilienza cyber per la PA. L'Agenzia ha, inoltre, adottato degli atti volti alla definizione del quadro organizzativo volto all'attuazione dell'investimento, nonché alla distribuzione dei fondi assegnati. Tra questi rientrano, in particolare, la Determina per l'adozione di un modello organizzativo in attuazione delle linee guida poste dalla Commissione europea e dalle autorità competenti e la Determina di assegnazione delle risorse per la realizzazione dei Centri di Valutazione del Ministero dell'Interno e della Difesa, nonché per la realizzazione degli interventi di potenziamento *cyber-defence*.

Per quanto riguarda, invece, il Comitato tecnico-scientifico di cui all'articolo 7, comma 1-*bis*, esso è istituito presso l'Agenzia e la relativa composizione e organizzazione sono stati definiti nel richiamato Regolamento di organizzazione e funzionamento. In attuazione di tale norma, all'articolo 11 del Regolamento è stata disciplinata la normativa di dettaglio relativa al predetto Comitato, individuandone le tipologie di componenti, i requisiti professionali richiesti per farne parte, le modalità di nomina e i profili organizzativi delle riunioni. In particolare, il Comitato è composto da rappresentanti dell'Agenzia, dell'industria, dell'accademia e dell'associazionismo di settore.

I componenti sono designati con decreto del Presidente del Consiglio dei ministri, sentito il Comitato di Vertice, su proposta del Direttore generale, restano in carica per due anni e possono essere rinnovati, con la medesima procedura, per un ulteriore anno.
Con DPCM del 15 giugno 2022 sono stati designati i 9 componenti del Comitato tecnico-scientifico, segnatamente:
- in rappresentanza dell'industria operativa negli ambiti di attività dell'Agenzia, comprese le piccole e medie imprese: Domitilla Benigni – Amministratore Delegato della Elettronica SpA e Presidente della Cy4Gate SpA; Paolo Dal Cin – Global Lead di Accenture Security; Massimo Enrico Proverbio – Chief IT Digital & Innovation Officer di Intesa Sanpaolo SpA; Franco Ongaro – Chief Technology & Innovation Officer del gruppo Leonardo SpA;
- in rappresentanza del sistema dell'università e della ricerca: Marco Conti – Direttore dell'Istituto di informatica e telematica del Consiglio Nazionale delle Ricerche e responsabile del Registro.it; Alessandro Curioni – IBM Fellow, Vice-President Europa e Africa nonché Direttore del Laboratorio di Ricerca IBM di Zurigo e Global Research VP IBM in Security e in Future of computing; Paola Severino – Professore emerito, Vice Presidente della Università LUISS Guido Carli e Direttore della Scuola Nazionale dell'Amministrazione; Donatella Sciuto – Professore ordinario di Ingegneria Informatica del Politecnico di Milano, nonché dal 2015 Prorettore vicario con delega alla ricerca;
- in qualità di esponente di associazioni del settore della sicurezza delle aziende strategiche del Paese, Andrea Chittaro.

La prima riunione del Comitato tecnico-scientifico si è svolta il 6 luglio 2022.

Sempre nell'ambito dello sviluppo di capacità, può farsi rientrare la funzione di cui alla lettera *m-bis*), che dispone l'assunzione, da parte dell'Agenzia per la cybersicurezza nazionale, di iniziative idonee a valorizzare la crittografia come strumento di cybersicurezza, anche tramite l'attivazione di ogni iniziativa utile al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, nonché valorizzando lo sviluppo di algoritmi proprietari e la ricerca e il conseguimento di nuove capacità crittografiche nazionali. A tal riguardo, l'Agenzia ha provveduto ad assumere, con le menzionate procedure concorsuali, dei tecnici crittografi che hanno avviato le attività volte all'attuazione di tale competenza.

Promozione della consapevolezza in materia di cybersicurezza

In relazione alle funzioni di cui alla lettera u), che riguardano attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia, fin dai primi mesi di attività dell'Agenzia sono state svolte campagne di sensibilizzazione. Al riguardo, la campagna divulgativa "I Navigati", realizzata a dicembre 2021 in collaborazione con il CERT-Fin, ABI Lab, Banca d'Italia e IVASS, nonché con il Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio dei ministri, è stata indirizzata ad un ampio pubblico e diffusa tramite canali televisivi e radiofonici.

Sempre negli ultimi mesi del 2021, è stata realizzata un'altra attività di sensibilizzazione, rivolta invece ad un pubblico mirato e, specificamente, al settore sanitario. Incentrata sui rischi cyber per il settore sanitario, la campagna è stata effettuata su scala nazionale ed è stata sviluppata e realizzata dall'ACN quale continuazione dell'iniziativa di *awareness* posta in essere con la Regione Lazio dopo gli attacchi ai danni dei sistemi informatici della stessa. La campagna nazionale è stata realizzata in concerto con gli uffici del Ministro per gli affari regionali e le autonomie e si è articolata su un ciclo di sei incontri, cui hanno preso parte i rappresentanti delle articolazioni sanitarie regionali, delle società che curano la gestione dei relativi servizi ICT, nonché delle aziende sanitarie locali e ospedaliere, per un totale di oltre 300 partecipanti.

Sviluppo della formazione e della crescita professionale

Per quanto riguarda le funzioni di cui alla lettera v), ai sensi della quale l'Agenzia promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, sono state avviate diverse attività di collaborazione. Ad esempio, è stata siglata un'intesa con la Regione Lazio per la collaborazione nel progetto di creazione di un centro regionale di formazione in materia di cybersicurezza ed è stata organizzata, in collaborazione con il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri, presso la Scuola nazionale dell'Amministrazione-SNA, una *Summer School* in materia di cybersecurity per alti dirigenti della Pubblica amministrazione italiana. É stato, inoltre, sottoscritto un Accordo di collaborazione per la costituzione di una rete di coordinamento degli istituti tecnologici per lo sviluppo della transizione digitale, per promuovere lo sviluppo di percorsi formativi dedicati alla digitalizzazione e alla sicurezza informatica dei processi delle imprese private e della Pubblica Amministrazione[13].

[13] L'Accordo è stato sottoscritto dal Ministro dell'Istruzione, dal Ministro per l'innovazione tecnologica e la transizione digitale, dall'Agenzia per la Cybersicurezza Nazionale, dalle Regioni Emilia-Romagna, Lombardia, Liguria, Puglia e Umbria, Confindustria, dall'Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa, l'Associazione Nazionale degli ITS, e dalla Fondazione Leonardo-Civiltà delle macchine.

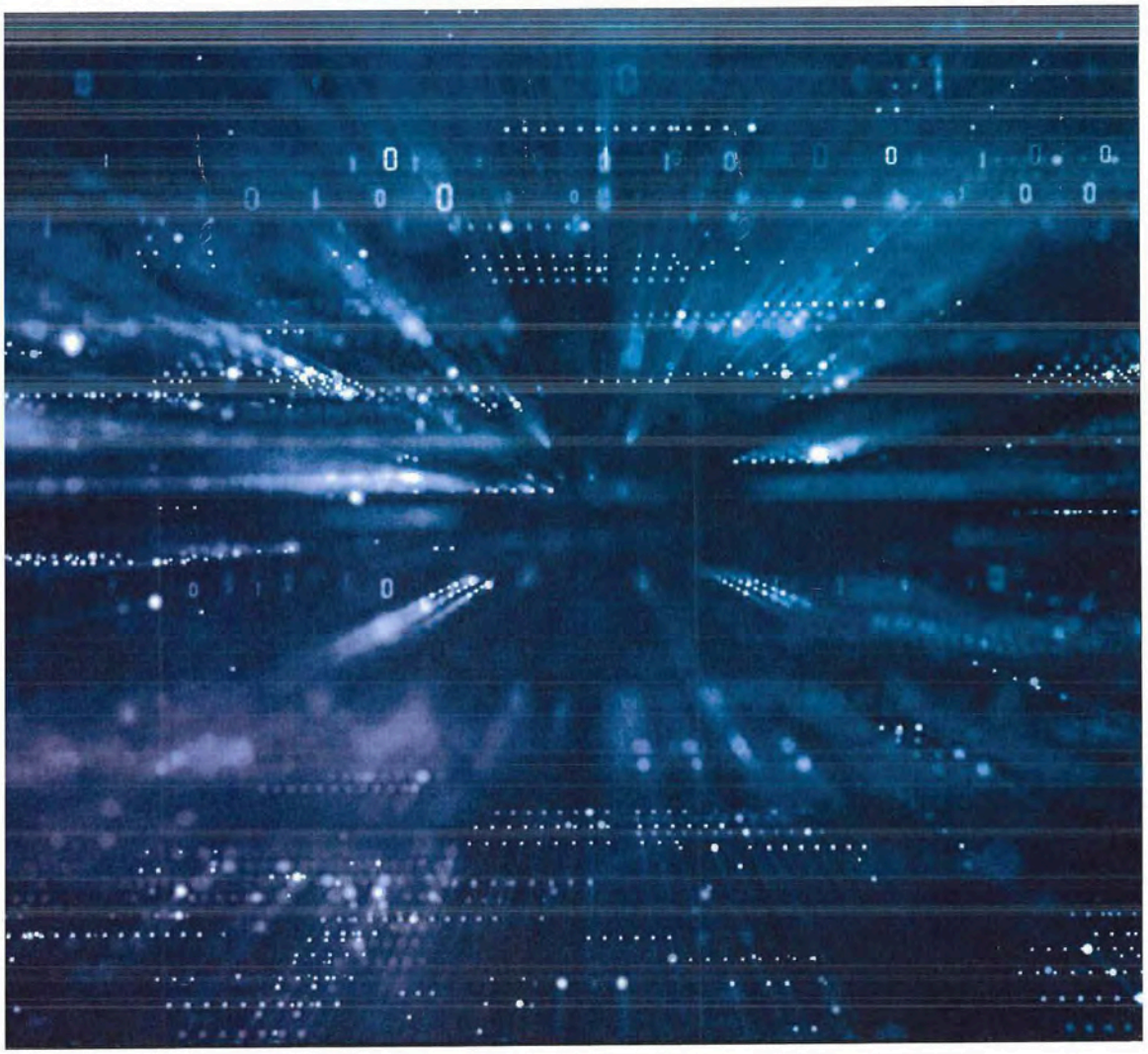
La norma in esame contempla, inoltre, la possibilità per l'ACN di avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati. A tal riguardo, è in corso di definizione il DPCM con il Ministero della difesa per l'utilizzo delle relative strutture che, in un'ottica di accelerazione e snellimento, è stato accorpato al DPCM concernente l'impiego di personale del Ministero della difesa presso l'ACN.

L'ACN si è, inoltre, dotata di capacità interne tese a esercitare un'azione di impulso e coordinamento dei lavori per l'adozione, in raccordo con il mondo accademico e con gli altri *stakeholder* pubblici e privati interessati, di un *framework* di regole comuni per la definizione e lo sviluppo di capacità e competenze nei settori avanzati della cybersicurezza. Ciò include l'obiettivo di migliorare i percorsi formativi scolastici, universitari e professionali, definendo, ad esempio, regole per la certificazione dei percorsi di studio che è necessario svolgere per acquisire le relative competenze sia a livello di istruzione post-secondaria di secondo grado, sia a livello universitario, post-universitario e professionale, nonché fornendo supporto metodologico per la definizione di programmi formativi dedicati, con diversi livelli di specializzazione in *cybersecurity*.

Collaborazioni istituzionali

Infine, il decreto-legge disciplina in più parti le collaborazioni istituzionali dell'Agenzia.

A tal riguardo, particolare rilievo assume quanto previsto dall'articolo 7, comma 5 , che disciplina la collaborazione tra l'Agenzia per la cybersicurezza nazionale e l'Autorità Garante per la protezione dei dati personali (GPDP), contemplando anche la possibilità di stipulare appositi protocolli d'intenti. Tale previsione è stata attuata il 26 gennaio 2022 con la sottoscrizione, da parte del Presidente del GPDP e il Direttore generale dell'ACN di un Protocollo di intesa per lo scambio di informazioni e la promozione di buone pratiche di sicurezza cibernetica, promuovendo altresì l'adozione di iniziative congiunte nel campo della cybersicurezza nazionale e della protezione dei dati personali.



4. IL NUCLEO PER LA CYBERSICUREZZA - NCS

PAGINA BIANCA

Il Nucleo per la Cybersicurezza - NCS

Gli artt. 8, 9 e 10 del decreto-legge sono dedicati al Nucleo per la cybersicurezza (NCS) disciplinandone, per la prima volta con norma di rango primario, finalità, composizioni, funzionamento e compiti, sia in via ordinaria che in caso di crisi di natura cibernetica. Il Nucleo è istituito in via permanente presso l'ACN e presieduto dal suo Direttore generale – o, per sua delega, dal Vice Direttore generale – e rappresenta la sede principale di coordinamento interistituzionale a livello tattico-operativo a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, con particolare riferimento agli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. Il NCS rappresenta, dunque, la sede privilegiata in cui ordinariamente si svolge il coordinamento interistituzionale tra le pubbliche amministrazioni individuate dall'articolo 8 del decreto-legge.

Essendo istituito presso l'Agenzia, quest'ultima svolge, ai sensi dell'articolo 7, comma 1, lettera c), del decreto-legge, attività di supporto al funzionamento del Nucleo.

Il Nucleo per la cybersicurezza è composto, ordinariamente, dal Consigliere militare del Presidente del Consiglio, dai rappresentanti di DIS, AISE e AISI, dei Ministeri che siedono nel CIC e del Dipartimento della protezione civile, nonché, per gli aspetti relativi alla trattazione di informazioni classificate, da un rappresentante dell'Ufficio centrale per la segretezza (UCSe) del DIS. Nelle situazioni di crisi di natura cibernetica (articolo 10), il Nucleo può essere integrato, in ragione della necessità, con un rappresentante del Ministero della salute e del Ministero dell'interno-Dipartimento dei vigili del fuoco, del soccorso pubblico e della difesa civile.

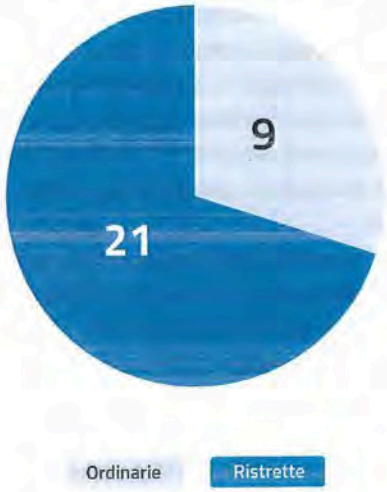
Al fine di consentire la costituzione del Nucleo e garantirne il corretto e ordinato funzionamento, le citate amministrazioni – anche in continuità con l'esperienza maturata dal precedente Nucleo per la sicurezza cibernetica che, ai sensi del DPCM 17 febbraio 2017, operava presso il Dipartimento delle informazioni per la sicurezza – hanno provveduto a nominare i propri qualificati rappresentanti presso il Nucleo.

L'Agenzia per la cybersicurezza nazionale, fin dal primo mese di operatività ha svolto tutte le previste attività di supporto al funzionamento del Nucleo. La prima riunione si è tenuta, infatti, circa 15 giorni dall'avvio iniziale dell'operatività dell'Agenzia (1° settembre 2021), presso la sede dell'ACN, in composizione ristretta, ovvero con la sola partecipazione dei rappresentanti delle amministrazioni e dei soggetti interessati alle tematiche all'ordine del giorno, secondo quanto previsto dall'articolo 8, comma 4 del medesimo decreto-legge. Il Nucleo si è, poi, regolarmente riunito con cadenza mensile, salvo nel caso in cui siano emerse situazioni tali da rendere opportuna una specifica convocazione. Ciò è avvenuto sia tramite determinazione del Presidente stesso, che su richiesta delle amministrazioni partecipanti. Dal 1° settembre 2021 al 30 settembre 2022, il NCS si è riunito 9 volte in composizione ordinaria, di cui due nel 2021, e 21 volte in

composizione ristretta, di cui cinque nel 2021 e sedici nel 2022. In linea con i compiti di cui sopra, le numerose riunioni del Nucleo hanno trattato tematiche attinenti alla gran parte delle diverse funzioni attribuite dall'articolo 9, contribuendo, in tal modo, a rendere efficaci e attuate le disposizioni del decreto-legge.

Difatti, sono stati affrontati argomenti sia di policy – attinenti, ad esempio, ad aggiornamenti su atti normativi in via di definizione a livello europeo – sia tecnici, tra cui indicatori di compromissione da sottoporre all'attenzione delle amministrazioni presenti. In particolare, l'attività del Nucleo si è intensificata a seguito dell'evoluzione dello scenario geopolitico connesso con il conflitto in Ucraina, per cui si sono tenute alcune riunioni con più di 50 operatori privati dei settori energetico, telecomunicazioni ed economico-finanziario, considerati i più sensibili rispetto alla situazione internazionale. Ciò al fine sia di sensibilizzare sull'accresciuto stato di allerta relativo a rischi di attacchi cyber, sia di acquisire elementi, anche al fine di aggiornare il punto di situazione, circa eventuali attacchi a loro danno. Con le medesime finalità sono state promosse, attraverso il Nucleo, la programmazione e la pianificazione operativa delle attività di risposta a situazioni di crisi cibernetica, in particolare in sede di Nucleo in composizione ristretta.

RIUNIONI NCS AL 30 SETTEMBRE 2022




Relazione al Parlamento
sullo stato di attuazione del decreto-legge 14 giugno 2021, n. 82 Nazionale di Cybersicurezza
ACN

conclusione

Conclusione

Nonostante la nuova architettura istituzionale cyber sia entrata in vigore da poco più di anno, sono già stati raggiunti significativi obiettivi in termini di attuazione del decreto-legge n. 82/2021. Difatti, come si è visto, ove non completata, è stato comunque dato – nonostante i numeri esigui di personale, essendo partiti da un piccolissimo nucleo di persone al 1° settembre 2021, progressivamente ampliato e in costante aumento per arrivare ai numeri previsti dalla legge istitutiva – almeno l'avvio all'attuazione di tutte le previsioni normative in esso contenute.
Al contempo, rimangono importanti traguardi da raggiungere, relativi alle previsioni del decreto-legge e alla Strategia nazionale di cybersicurezza, nonché all'ambito delle progettualità PNRR, che risultano ancora più sfidanti se considerati alla luce del contesto internazionale sopra descritto.

In particolare, l'attuazione della Strategia nazionale di cybersicurezza 2022-2026 e, nello specifico, delle 82 misure previste nel correlato Piano di implementazione, rappresenta un'ambiziosa – ma concreta – linea d'azione per gli anni a venire, così da poter arrivare, alla fine del quinquennio, ad un rafforzamento della resilienza nella transizione digitale del sistema Paese, che promuova un uso sicuro delle tecnologie, indispensabili per la nostra prosperità economica, presente e futura, al conseguimento dell'autonomia strategica nella dimensione cibernetica, all'anticipazione dell'evoluzione della minaccia cyber, alla gestione di crisi cibernetiche in scenari geopolitici complessi, nonché al contrasto della disinformazione online, nel rispetto dei diritti umani, dei nostri valori e principi.

> *Ciò richiederà la prosecuzione del forte impegno in tale settore, anche grazie ad un importante sostegno da parte del Parlamento, con particolare riferimento a quelle misure che si potrebbero adottare al fine di agevolare la piena realizzazione dell'architettura nazionale e l'ulteriore rafforzamento della resilienza e della cybersicurezza nazionali, specie in un contesto in costante evoluzione che richiede aggiornamento normativo, fondi, ricerca, innovazione, consapevolezza e cultura della cybersicurezza. Scenario questo che richiede, in un'ottica di sicurezza nazionale nello spazio cibernetico, anche l'adozione di ulteriori e idonee iniziative di tutela in materia di acquisizione e dispiegamento delle tecnologie emergenti.*

PAGINA BIANCA

190270012910