Senato della Repubblica

Servizio per la qualità degli atti normativi

Osservatorio sull'attuazione degli atti normativi

Focus

Relazione sull'attività svolta dall'Agenzia per la cybersicurezza nazionale

XIX legislatura

febbraio 2023

n. 1

Relazioni alle Camere

INDICE

L'OBBLIGO DI RELAZIONE AL PARLAMENTO 5

IL QUADRO NORMATIVO DI RIFERIMENTO 5

L'APPARATO ORGANIZZATIVO NAZIONALE IN TEMA DI CYBERSICUREZZA 6

LE ATTIVITÀ DELL'AGENZIA 7

I PROFILI FINANZIARI 9

OSSERVAZIONI 9

L'OBBLIGO DI RELAZIONE AL PARLAMENTO

L'Agenzia per la cybersicurezza nazionale[1] è stata istituita dall'articolo 5 del decreto-legge 14 giugno 2021, n. 82[2], con il compito di assicurare «*il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale*» e di promuovere «*la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore*»[3].
L'Agenzia si è costituita il 1° settembre 2021.
Il 5 dicembre 2022 è stata presentata al Parlamento la prima Relazione sulle attività svolte dall'Agenzia nell'anno precedente, riferita al periodo dal 1° settembre al 31 dicembre 2021.
In sede di prima applicazione, il termine per la trasmissione della relazione è stato fissato al 30 novembre 2022[4], mentre il termine ordinario è il 30 aprile di ogni anno[5]. La Relazione (Doc. CCXVIII, n. 1) è stata assegnata in Senato alla 1ª Commissione permanente.

IL QUADRO NORMATIVO DI RIFERIMENTO

Il coordinamento delle «*attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali*» è un compito inizialmente attribuito al Dipartimento delle informazioni per la sicurezza (DIS) della Presidenza del Consiglio dei Ministri[6]. L'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, è stata definita in dettaglio con decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013[7], che ha istituito presso il DIS il Nucleo per la sicurezza cibernetica, incaricato della prevenzione e gestione di eventuali situazioni di crisi, nonché dell'attivazione delle procedure di allertamento. Questo modello organizzativo-funzionale è stato aggiornato con DPCM 17 febbraio 2017 a seguito delle novità introdotte dalla «direttiva NIS[8]».
L'assetto del sistema nazionale di sicurezza cibernetica è stato profondamente ridefinito dal decreto-legge n. 82 del 2021. Nel nuovo quadro normativo, l'istituzione dell'Agenzia è strumentale all'esercizio delle competenze di alta direzione e responsabilità delle politiche

[1] Di seguito denominata «Agenzia».
[2] Convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.
[3] Articolo 7, comma 1, lett. a), del decreto-legge n. 82 del 2021.
[4] Articolo 17, comma 10-*bis*, del decreto-legge n. 82 del 2021.
[5] Articolo 14, comma 1, del decreto-legge n.82 del 2021.
[6] Articolo 3, legge 7 agosto 2012, n. 133, Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto.
[7] "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".
[8] 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 nell'Unione, recepita con il decreto legislativo 18 maggio 2018, n. 65. La direttiva NIS è stata abrogata e sostituita dalla direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione ("direttiva NIS 2").

di cybersicurezza e di adozione della Strategia nazionale di cybersicurezza attribuite al Presidente del Consiglio dei ministri. A tal fine, è stato disposto il trasferimento dal DIS all'Agenzia di funzioni, beni strumentali e documentazione in materia di cybersicurezza[9].
Lo stato di attuazione, al 30 settembre 2022, delle disposizioni in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, anche al fine di formulare eventuali proposte in materia, è oggetto di uno specifico obbligo di relazione del Governo al Parlamento (art. 17, comma 10-*bis*, lettera b), del decreto-legge n. 82 del 2021). La Relazione, per la quale era previsto il termine del 31 ottobre 2022, è stata presentata il 18 novembre e assegnata in Senato alla 1ª Commissione permanente (doc. XXVII n. 1).

L'APPARATO ORGANIZZATIVO NAZIONALE IN TEMA DI CYBERSICUREZZA

La Relazione sull'attività svolta dall'Agenzia illustra l'ecosistema nazionale di cybersicurezza come ridisegnato dal decreto-legge n. 82 del 2021. Il sistema è composto dal Presidente del Consiglio dei ministri; dall'Autorità delegata per la sicurezza della Repubblica, ove istituita e per le sole funzioni non attribuite in via esclusiva al Presidente del Consiglio; dal Comitato interministeriale per la cybersicurezza (CIC) istituito presso la Presidenza del Consiglio dei ministri, con compiti di consulenza, proposta e vigilanza; dai Ministeri e istituzioni con competenze trasversali in ambito *cyber*; dal Nucleo per la cybersicurezza (NCS) istituito presso l'Agenzia, con funzioni di supporto per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi; dagli operatori economici privati, università, enti di ricerca e società civile, che prendono parte al sistema tramite lo strumento del partenariato pubblico-privato; dall'Agenzia per la cybersicurezza nazionale (ACN), designata quale Autorità nazionale per la cybersicurezza, che è deputata alla tutela dello spazio cibernetico.
Sotto la responsabilità del Presidente del Consiglio dei ministri, l'Agenzia assicura, all'interno dell'ecosistema nazionale di cybersicurezza, un'azione di coordinamento che coinvolge tutte le Amministrazioni con competenza in materia di sicurezza cibernetica e resilienza (Forze di polizia, Ministero della difesa, organismi di informazione per la sicurezza, Ministero degli affari esteri e della cooperazione internazionale) e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetica.
L'Agenzia è, inoltre, l'autorità nazionale competente che detiene le funzioni regolamentari di certificazione, ispezione, vigilanza e sanzionatorie per l'attuazione della normativa relativa al Perimetro di sicurezza nazionale cibernetica[10], centro nazionale di coordinamento in attuazione del regolamento (UE) 2021/887 e soggetto attuatore per la

[9] Con decreto del Presidente del Consiglio dei ministri del 16 settembre 2021.
[10] Il decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni, dalla legge 18 novembre 2019, n. 133 («Decreto Perimetro») ha istituito il perimetro di sicurezza nazionale cibernetica al «*fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativo e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale*».

realizzazione dell'investimento 1.5 *Cybersecurity*, Missione 1 - componente 1 del Piano nazionale di ripresa e resilienza (PNRR).
Il 18 maggio 2022, il Comitato interministeriale per la cybersicurezza ha approvato la Strategia nazionale di cybersicurezza (2022-2026) e l'annesso Piano di implementazione, elaborati dall'Agenzia.

LE ATTIVITÀ DELL'AGENZIA

L'Agenzia ha avviato le proprie attività il 1° settembre 2021, acquisendo e razionalizzando funzioni, risorse umane, beni e dotazioni di una pluralità di soggetti istituzionali, al fine di conferire unitarietà di indirizzo e azione alle politiche in materia di cybersicurezza. Il trasferimento di personale del DIS, integrato dal personale messo a disposizione dalle altre amministrazioni dello Stato, ha consentito l'immediata operatività dell'Agenzia. Sono state inoltre trasferite presso l'Agenzia le funzioni del *Computer security incident response team* (CSIRT Italia), la struttura tecnica di prevenzione, coordinamento e risposta agli eventi e incidenti informatici con impatto sul territorio nazionale; dell'Organismo di certificazione della sicurezza informatica (OCSI), che emette su richiesta volontaria dei produttori del settore *Information and Communication Technologies* certificazioni di sicurezza cibernetica su prodotti ICT e del Centro di valutazione e certificazione nazionale (CVCN), che si occupa di effettuare valutazioni per l'impiego di categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica.
Nell'esercizio della sua autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, l'Agenzia ha adottato regolamenti interni e ha provveduto alla migrazione dei dati di propria competenza e alla progettazione del *data center*, dei sistemi IT e dei portali *internet*. Il 30 dicembre 2021 è stata attivata la Funzione certificazioni e vigilanza, che cura le attività ispettive e di verifica; è stato, inoltre, costituito l'Organo centrale di sicurezza per la trattazione e la gestione della documentazione classificata ai sensi del decreto del Presidente del Consiglio dei ministri 6 novembre 2015.
L'Agenzia elabora pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza e fornisce supporto tecnico al Gruppo di coordinamento che cura le istruttorie per l'applicazione dei poteri speciali[11], per quanto attiene a operazioni societarie che riguardino reti di telecomunicazione a banda larga con tecnologia 5G e operazioni societarie che comportino un impatto su attivi strategici in ambito ICT e di cybersicurezza.
In ambito *cyber* i maggiori rischi di tipo sistemico sono gli attacchi in grado di arrestare l'erogazione di servizi essenziali di un Paese, l'affidabilità e la robustezza della catena di approvvigionamento tecnologico e i tentativi di ingerenza e destabilizzazione del dibattito pubblico con campagne di disinformazione. In tale ambito l'Agenzia opera mediante il CSIRT-Italia nella direzione preventiva e reattiva. In particolare, nella direzione preventiva si individuano attraverso il monitoraggio della rete *internet* i rischi e gli incidenti a danno

[11] C.d. "*Golden power*".

di soggetti pubblici e privati[12], mentre nella direzione reattiva si gestiscono gli eventi sottoposti al CSIRT-Italia dai soggetti interessati.
Tra le minacce più insidiose per l'operatività delle vittime, soprattutto per quelle del settore privato, la Relazione invidua il *ransomware*[13], ovvero la situazione nella quale l'attaccante cifra i dati di un'organizzazione e minaccia i titolari di tali dati, ma anche soggetti terzi (clienti, fornitori, *partner*), di pubblicarli al fine di ottenere un riscatto. Secondo l'Agenzia europea per la cybersicurezza, l'Italia è il quarto Paese al mondo più colpito da tale minaccia. Le vittime di questi eventi appartengono per l'85% al settore privato, prevalentemente grandi imprese del settore manifatturiero, e per il 15% al settore delle pubbliche amministrazioni, principalmente enti locali.
La Relazione fa riferimento anche alle *cyber gang*, organizzazioni criminali che si caratterizzano per la capacità di operare lungo tutta la filiera dell'attacco, dalla scelta della vittima, all'intrusione nel sistema informatico, all'utilizzo di strumenti di infezione sviluppati in proprio, fino alla richiesta e negoziazione del riscatto. Rispetto alle attività delle *cyber gang*, l'Agenzia interviene con la divulgazione delle pratiche di prevenzione, la preparazione a situazioni di crisi, le procedure di allertamento e le risposte agli incidenti.
La prevenzione delle situazioni di crisi e l'attivazione delle procedure di allertamento e della preparazione della gestione sono affidate al Nucleo per la cybersicurezza, presieduto dal direttore generale dell'Agenzia e composto dal Consigliere militare del Presidente del Consiglio dei ministri, dai rappresentanti del DIS, dell'AISE e dell'AISI, dei Ministeri rappresentati nel Comitato interministeriale per la cybersicurezza e del Dipartimento della protezione civile. Il Nucleo è stato convocato già nel corso del breve periodo di attività dell'Agenzia, anche in occasione della diffusione mondiale di una vulnerabilità critica del prodotto Log4J di Apache Foundation. In particolare, nel periodo 1° settembre-31 dicembre 2021, il Nucleo per la cybersicurezza si è riunito in composizione ordinaria e in composizione ristretta per un totale di sette volte.
Nel contesto internazionale in materia *cyber*, l'Agenzia opera in raccordo con il Ministero degli affari esteri e della cooperazione internazionale. Tra le principali attività svolte, la Relazione ricorda la partecipazione dell'Agenzia al Gruppo di lavoro interministeriale sul *cybercrime* delle Nazioni Unite, volto a definire la posizione nazionale nell'ambito dei negoziati della Convenzione internazionale sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione ai fini criminali che si è tenuta a New York dal 17 al 28 gennaio 2022. L'Agenzia ha condiviso le esperienze nazionali in materia di gestione degli incidenti e di crisi cibernetiche con la NATO, al fine di consolidare le interlocuzioni di vertice sul tema delle strategie nazionali di *cybersicurezza*. In ambito europeo, l'Agenzia ha partecipato ai lavori dell'*Horizontal Working Party on Cyber Issues*-HWPCI, istituito presso il Consiglio dell'unione europea per l'elaborazione e l'implementazione delle politiche pubbliche in tema di *cybersicurezza*.

[12] Le statistiche e le tipologie di incidenti *cyber* sono pubblicate nelle pagine da 26 a 31 della Relazione.
[13] Per approfondimenti si rinvia alle statistiche degli interventi e delle tipologie di incidenti di cui alle pagine 26, 27 e 29 della Relazione.

I PROFILI FINANZIARI

La dotazione finanziaria dell'Agenzia è stata disposta dall'articolo 18 del decreto-legge n. 82 del 2021, con 41.000.000 di euro per il 2022 e 70.000.000 di euro per l'anno 2023 e una dotazione annuale crescente fino ai 122.000.000 di euro a decorrere dal 2027. Sono previsti ulteriori stanziamenti, da determinare all'interno della legge di bilancio, per la realizzazione di progetti specifici.
L'Agenzia ha aderito al Protocollo d'intesa con tutte le autorità amministrative indipendenti per la gestione in comune delle procedure di appalto, per l'acquisizione di lavori, servizi e forniture, conseguendo risparmi di spesa. Alle entrate dell'Agenzia contribuiscono anche i corrispettivi ricevuti per servizi prestati a soggetti pubblici e privati; i proventi derivanti dalle invenzioni dai prodotti dell'ingegno dell'Agenzia; i proventi derivanti dalle sanzioni irrogate; i contributi dell'Unione europea e di organismi internazionali anche a seguito della partecipazione a bandi, progetti e programmi di collaborazione e le risorse del PNRR (Missione 1 - componente 1), investimento 1.5, pari a 623.000.000 euro.

OSSERVAZIONI

La Relazione dell'Agenzia per la cybersicurezza nazionale non contiene dati e informazioni sui soggetti maggiormente colpiti dagli attacchi, neanche in forma aggregata; a tal proposito, potrebbe essere utile un approfondimento dedicato agli attacchi subiti dalle pubbliche amministrazioni. Quanto ai rischi *cyber*, la Relazione offre un approfondimento solo sugli attacchi *ransomware*, trascurando le altre modalità di aggressione. Sarebbe utile, inoltre, l'inserimento di statistiche sulla distribuzione geografica di attacchi e incidenti per tutti i settori e per tutti i tipi di minaccia, con l'indicazione delle misure di sicurezza specifiche per ciascuna tipologia di aggressione.
Come evidenziato nella Relazione sull'attuazione del decreto-legge n. 82 del 2021, tutte le funzioni e attività in materia di tutela della sicurezza e della resilienza nello spazio cibernetico attribuite all'Agenzia risultano quantomeno avviate. La piena realizzazione dell'architettura nazionale e l'ulteriore rafforzamento della resilienza e della cybersicurezza nazionali potrebbero richiedere nuove iniziative, in particolare modifiche normative o stanziamenti di risorse, da sottoporre all'approvazione del Parlamento.
All'Agenzia sono affidati numerosi compiti connessi all'attuazione della Strategia nazionale di cybersicurezza 2022-2026 e delle 82 misure descritte dal Piano di implementazione. La prossima Relazione annuale, da presentare entro il 30 aprile, potrà fornire informazioni utili sullo stato di attuazione della Strategia.

Senato della Repubblica

Servizio per la qualità degli atti normativi

Osservatorio sull'attuazione degli atti normativi

Cons. Lorella Di Giambattista

tel. 06 6706 3437
email quan@senato.it