Le novità introdotte dal Decreto-legge 82/2021 convertito: la nuova governance istituzionale di cybersicurezza e l'Agenzia per la cybersicurezza nazionale

Lorenzo Desidera
Dottore in Ingegneria gestionale, Director Cybersecurity & Privacy di PwC Italy

Maria Chiara Curinga
Dottoressa in Ingegneria gestionale, Manager Cybersecurity & Privacy di PwC Italy

Christian Ferrari
Dottore in Giurisprudenza e in Economia e Management, Senior Associate Cybersecurity & Privacy di PwC Italy

1. La nuova architettura istituzionale e la riorganizzazione del quadro normativo della cybersicurezza nazionale

Il numero in crescita esponenziale di attacchi cibernetici negli ultimi 15 anni, a danno di soggetti pubblici e privati, ha reso necessario un intervento sul piano istituzionale, al livello nazionale ed europeo, atto a favorire lo sviluppo di capacità di prevenzione e risposta agli incidenti di cybersicurezza. Tale intervento, articolato attraverso la definizione di strategie di *cybersecurity* di medio-lungo periodo, la strutturazione di una *governance* sui temi di cybersicurezza e la definizione di un quadro normativo di riferimento, ha subìto una recente rapida evoluzione causata, in maniera prevalente, dal *black swan*[1] pandemico, che ha accelerato il processo della c.d. "transizione digitale" e mostrato come il *cyberspace*, mai come prima d'ora, sia vitale per lo svolgimento di qualsiasi attività umana (dal lavoro all'apprendimento, fino alla socializzazione) e, più in

[1] Sul concetto di "*black swan*" e la correlazione con le attività di *risk management* si veda l'articolo di C. Brooks, *Risk management and black swan events*, in forbes.com, 23 ottobre 2019, disponibile all'indirizzo: https://www.forbes.com/sites/cognitiveworld/2019/10/23/risk-management-and-black-swan-events/.

generale, essenziale per il mantenimento delle attività economiche, sociali e civili fondamentali.

In tale contesto si innesta la recente approvazione (e successiva conversione) del Decreto-legge 14 giugno 2021, n. 82 recante "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*"[2] (di seguito anche "decreto-legge" o "D.L. 82/2021 convertito").

Tale decreto-legge ridefinisce la *governance* istituzionale e riorganizza il quadro normativo nazionale in materia di cybersicurezza, istituendo per la prima volta un'agenzia pubblica specializzata ("l'Agenzia per la cybersicurezza nazionale"), allineandosi a iniziative simili già adottate da altri paesi europei (quali, in particolare, Francia e Germania)[3], dedicata alla costruzione e allo sviluppo di capacità nazionali di resilienza cibernetica.

L'istituzione dell'Agenzia per la cybersicurezza nazionale e la nuova definizione e attribuzione di compiti e responsabilità agli ulteriori attori istituzionali coinvolti ridisegnano il quadro di *governance* nazionale, contribuendo all'effettiva applicazione del quadro normativo nazionale in materia di cybersicurezza (di introduzione relativamente recente nel contesto italiano).

Il tema imminente della gestione della sicurezza cibernetica sul piano sistemico, costituisce altresì uno degli interventi del Piano Nazionale di Ripresa e Resilienza (c.d. "PNRR"), trasmesso dal Governo alla Commissione europea il 30 aprile 2021; il primo intervento della missione 1 relativa alla "Digitalizzazione, innovazione, competitività, cultura e turismo" mira, infatti, a sostenere la transizione digitale del Paese e ad offrire a cittadini e imprese servizi efficaci, in sicurezza e pienamente accessibili.

In particolare, relativamente agli aspetti di *cybersercurity* il PNRR pone l'attenzione:

- sul rafforzamento dei presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio intercettatati verso la PA e le imprese di interesse nazionale;
- sulla costruzione o il consolidamento delle capacità tecniche di valutazione e *audit* continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale;

[2] Il decreto in parola è stato convertito, con modificazioni, dalla L. 4 agosto 2021, n. 109 e pubblicato nella G.U. n. 185 del 4 agosto 2021. Il testo in vigore alla data di stesura del presente articolo è disponibile al seguente indirizzo: www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg.

[3] Sul punto si veda l'articolo di F. Bechis, *Non solo cyber, così riformiamo l'intelligence. Parla Franco Gabrielli*, in formiche.net, 14 agosto 2021, disponibile all'indirizzo: https://formiche.net/2021/08/non-solo-cyber-cosi-riformiamo-lintelligence-parla-franco-gabrielli/.

- sull'irrobustimento degli *asset* e delle unità *cyber* incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*.

A tale intervento sono destinati investimenti per circa 620 milioni di euro[4], distribuiti nel quadriennio 2021-2024. Tali sovvenzioni, lette in combinato disposto con le *milestones* di intervento trasmesse dal governo alla Commissione europea, daranno un impulso determinante nell'attuazione effettiva della nuova *governance* istituzionale e alle funzioni della neonata Agenzia per la cybersicurezza nazionale.
Alla luce dell'articolato quadro descritto, i temi trattati nei paragrafi successivi analizzano le due principali direttrici, tra loro strettamente correlate, sottese all'introduzione del D.L. 82/2021 convertito, esplicitate già nell'*incipit* del decreto-legge stesso:

- da un lato, la necessità di ridefinire la *governance* istituzionale di cybersicurezza;
- dall'altro lato, la necessità di riorganizzare il quadro normativo nazionale applicabile in materia di cybersicurezza.

2. La ridefinizione dell'architettura istituzionale della cybersicurezza ad opera del D.L. 82/2021 convertito

La prima direttrice sottesa all'introduzione del D.L. 82/2021 convertito è volta a ridefinire l'architettura istituzionale di cybersicurezza nazionale, elemento che ne rappresenta, di fatto, la finalità principale: la quasi totalità degli articoli del decreto, infatti, pur da diverse prospettive (e con livelli di dettaglio diversi), contiene disposizioni atte a stabilire nuovi attori istituzionali e ad attribuire ruoli e responsabilità specifiche ad attori e organismi già esistenti e coinvolti nella gestione della cybersicurezza nazionale[5].

[4] Di cui 241 milioni di euro destinati alla creazione di una infrastruttura nazionale per la cybersicurezza, 231 milioni di euro destinati al rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica; 150 milioni di euro per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'interno, Difesa, Guardia di Finanza e Consiglio di Stato. Per ulteriori approfondimenti si veda il PNRR redatto dal Governo italiano, consultabile all'indirizzo: https://www.governo.it/sites/governo.it/files/PNRR.pdf e il *dossier* redatto dal Servizio Studi della Camera dei Deputati e del Senato della Repubblica "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", disponibile all'indirizzo: https://www.senato.it/service/PDF/PDFServer/BGT/01306371.pdf.
[5] Da questa prospettiva è rilevante quanto riportato nell'*incipit* del decreto-legge convertito, in cui si sottolinea, a più riprese, la "straordinaria necessità e urgenza (…) di razionalizzare le competenze in materia" e la necessità di "intervenire con urgenza al fine di ridefinire l'architettura italiana di cybersicurezza".

La ridefinizione dell'architettura istituzionale di cybersicurezza contenuta nel decreto-legge si sostanzia in una serie di interventi finalizzati a riordinare i diversi ambiti di operatività della cybersicurezza nazionale (ambiti correlati, ma comunque distinti) e propedeutici, da un lato, allo sviluppo di capacità di resilienza cibernetica nazionale e, dall'altro lato, allo svolgimento di attività di "*cyber-intelligence* (di competenza degli organismi di informazione per la sicurezza), di *cyber-defense* (intesa come difesa e sicurezza militare dello Stato, di competenza del Ministero della difesa) e alla prevenzione e repressione dei reati (di competenza delle Forze di polizia)"[6].

Nel nuovo quadro di governance di cybersicurezza definito dal decreto-legge, al Presidente del Consiglio dei ministri, posto al vertice dell'architettura istituzionale, sono attribuiti poteri in via esclusiva[7] tra cui, in particolare, l'alta direzione e la responsabilità generale delle politiche di cybersicurezza e l'adozione della strategia nazionale di cybersicurezza (a cui si aggiungono i poteri di nomina e revoca del direttore generale e del vice direttore generale dell'istituenda Agenzia, previa deliberazione del Consiglio dei ministri) e poteri attribuiti in via non esclusiva, eventualmente demandati all'Autorità delegata[8], ove istituita.

In ausilio all'esercizio dei poteri attribuiti al Presidente del Consiglio dei ministri e all'Autorità delegata (ove istituita), il decreto-legge prevede l'istituzione di due ulteriori soggetti istituzionali: il Comitato Interministeriale per la Cybersicurezza (di seguito anche "CIC") e l'Agenzia per la cybersicurezza nazionale (di seguito anche "Agenzia" o "ACN").

Secondo quanto disposto dall'articolo 4, comma 1, del decreto-legge, presso la Presidenza del Consiglio dei ministri è istituito il CIC, quale organo "con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza". Il CIC, nella sostanza, anche in ottica di attuazione della ridefinizione dei diversi ambiti di operatività citati, acquisisce una funzione

[6] Sul punto si veda la Relazione redatta dalla Camera dei Deputati sul Disegno di legge presentato dal Presidente del Consiglio dei ministri e recante "*Conversione in legge del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenza per la cybersicurezza nazionale*". Il testo completo della relazione è consultabile al seguente indirizzo: http://documenti.camera.it/leg18/pdl/pdf/leg.18.pdl.camera.3161.18PDL0147140.pdf.

[7] Tra questi vi rientrano anche attribuzioni di carattere strumentale ai tre principali poteri attribuiti ossia l'approvazione di direttive per la cybersicurezza e l'emanazione di disposizioni necessarie per l'organizzazione e il funzionamento dell'istituenda Agenzia.

[8] Si fa riferimento alla facoltà attribuita al Presidente del Consiglio dei ministri di delegare alcune funzioni all'Autorità istituita ai sensi dell'art. 3 della legge 3 agosto 2007, n. 124. Le disposizioni del decreto-legge prevedono comunque che l'Autorità delegata informi costantemente il Presidente del Consiglio dei ministri sulle modalità di esercizio delle funzioni delegate, prevedendo anche l'ipotesi di eventuale avocazione dell'esercizio delle stesse.

quasi speculare a quella assunta dal Comitato Interministeriale per la Sicurezza della Repubblica (di seguito anche "CISR") incardinato nel Sistema di informazione per la sicurezza della Repubblica[9]; il CIC, tra l'altro, acquisisce la quasi totalità dei compiti precedentemente attribuiti al CISR dal decreto-legge 21 settembre 2019, n. 105 convertito[10]. Presieduto dal Presidente del Consiglio dei ministri, il CIC è composto dall'Autorità delegata e dai ministri coinvolti[11], nonché dal direttore generale dell'Agenzia che, all'interno del Comitato, assume il ruolo di segretario. Tra i compiti principali si rilevano, in particolare, l'attività di consulenza e proposta, al Presidente del Consiglio dei ministri, di indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale, nonché attività di alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza.

Il secondo attore istituzionale coinvolto nella nuova architettura nazionale di cybersicurezza, ossia l'Agenzia per la cybersicurezza nazionale, viene istituito "a tutela degli interessi nazionali nel campo della cybersicurezza", ai sensi dell'articolo 5, comma 1, del decreto-legge in analisi. L'Agenzia, si legge nel comma successivo del medesimo articolo, "ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria". A tal proposito, è opportuno rilevare lo sforzo del legislatore nella ricerca di un punto di equilibrio teso a garantire, da un lato, l'attribuzione di un'autonoma personalità giuridica all'Agenzia (che esercita le funzioni che le sono attribuite dal decreto tramite i propri organi e, in particolare, tramite il direttore generale che ne è anche legale rappresentante) la cui attività è incardinata, dall'altro lato, in un alveo di regole definito dal decreto-legge istitutivo e, di riflesso, posta in attuazione di quanto previsto dai regolamenti e dalle direttive impartite dal Presidente del Consiglio dei ministri e dall'Autorità delegata (per i poteri a questa demandati), che possono avvalersi dell'Agenzia per l'esercizio delle competenze a essi attribuite dal decreto-legge in parola[12]. L'autonomia dell'Agenzia e l'intervento governativo, inoltre, sono a loro volta ulteriormente limitati, in uno scacchiere di controlli incrociati, dall'attività

[9] Istituito, come noto, dalla legge 3 agosto 2007, n. 124 recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", disponibile all'indirizzo https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2007-08-13&atto.codiceRedazionale=007G0139&elenco30giorni=false.

[10] Fa eccezione quanto previsto dall'articolo 5 del decreto-legge perimetro, che continua ad attribuire al CISR il compito di deliberazione preventiva in caso di necessità di disattivazione, totale o parziale, di uno o più prodotti o apparati per rischi gravi e imminenti per la sicurezza nazionale, da parte del Presidente del Consiglio dei ministri.

[11] Il cui elenco di dettaglio è riportato all'articolo 4, comma 3, del decreto-legge.

[12] Come previsto dall'articolo 5, comma 2, del decreto-legge.

di controllo parlamentare tramite il Comitato Parlamentare per la Sicurezza della Repubblica ("COPASIR")[13].

All'interno dell'Agenzia sono, inoltre, fatti confluire tutti gli organismi nazionali istituiti dai precedenti interventi normativi in materia di cybersicurezza. In particolare, sono confluiti presso l'Agenzia: il Nucleo per la Cybersicurezza (già Nucleo per la Sicurezza Cibernetica), istituito dal D.P.C.M. del 24 gennaio 2013[14], il CSIRT Italia, istituito dal decreto legislativo 18 maggio 2018, n. 65 di recepimento della c.d. "Direttiva NIS" (e precedentemente incardinati presso il Dipartimento delle Informazioni per la Sicurezza – "DIS") e il Centro di Valutazione e di Certificazione Nazionale ("CVCN", precedentemente istituito presso l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione – "ISCTI" – del Ministero dello sviluppo economico).

L'Agenzia, inoltre, assume il ruolo di Autorità nazionale NIS e di Autorità nazionale di certificazione della cybersicurezza (secondo quanto previsto dal Regolamento UE sulla cybersicurezza[15]).

L'Agenzia, infine, acquisisce poteri e compiti precedentemente attribuiti alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico nell'ambito delle disposizioni istitutive del Perimetro di Sicurezza Nazionale Cibernetica, nonché le funzioni attribuite precedentemente all'AgID in materia di cybersicurezza.

2.1 L'Agenzia per la cybersicurezza nazionale: organizzazione, compiti e funzioni attribuiti

L'organizzazione dell'Agenzia e i relativi compiti e funzioni attribuiti sono disciplinati dalle disposizioni del D.L. 82/2021 convertito e dalle ulteriori direttive e regolamenti adottati dal Presidente del Consiglio dei ministri tramite D.P.C.M.

In merito all'organizzazione dell'Agenzia, occorre rilevare quanto previsto dall'articolo 6 del D.L. 82/2021 convertito, che ne prevede l'articolazione in

[13] Il COPASIR, per esempio, per quanto attiene ai poteri esercitabili dall'Agenzia in autonomia, può chiedere, per le materie di competenza, l'audizione del direttore generale; per quanto attiene, invece, all'esercizio del potere direttivo del Presidente del Consiglio dei ministri, è previsto che il COPASIR esprima pareri, per esempio, sui regolamenti relativi all'organizzazione e al personale dell'Agenzia.

[14] Pubblicato in Gazzetta Ufficiale n. 66 del 19 marzo 2013, disponibile all'indirizzo: www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.

[15] Il riferimento è al Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), disponibile al link: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32019R0881.

organi e *uffici*. Sono organi: i) il direttore generale, gerarchicamente sovraordinato al personale dell'Agenzia (che ricopre il ruolo di diretto referente nei rapporti con il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita); ii) il collegio dei revisori dei conti.

È prevista, inoltre, l'articolazione fino a un numero massimo di otto uffici di livello dirigenziale generale e fino a un massimo di trenta articolazioni di livello dirigenziale non generale.

Il decreto-legge prevede, infine, che sia demandata a ulteriori regolamenti[16] la definizione di disposizioni di dettaglio in merito all'organizzazione e al funzionamento dell'Agenzia, da adottare tramite decreto del Presidente del Consiglio dei ministri entro centoventi giorni dalla data di entrata in vigore della legge di conversione del D.L. 82/2021 convertito[17] previo parere del COPASIR e sentito il CIC.

Per quanto attiene, invece, al novero di compiti e funzioni attribuiti, occorre preliminarmente rammentare che all'Agenzia sono stati demandati, dal decreto-legge in analisi (precisamente, dall'articolo 7), compiti "inediti" nel contesto normativo nazionale e compiti, invece, "acquisiti", ossia destinati dal decreto-legge all'Agenzia e precedentemente attribuiti ad altri attori istituzionali.

Tra i compiti "inediti" affidati all'Agenzia si rilevano, in particolare: i) l'attività di coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale; ii) la promozione e 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; iii) il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore; iv) la cura e la promozione per la definizione e il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza (anche fornendo pareri non vincolanti su iniziative legislative e regolamentari); v) il coordinamento e la promozione, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, della cooperazione internazionale in materia di cybersicurezza.

Tra i compiti, invece, "acquisiti", ossia precedentemente attribuiti ad altri attori istituzionali, si rilevano, in particolare: i) funzioni attribuite all'Agenzia in qualità di Autorità nazionale competente e punto di contatto unico in

[16] È prevista, in particolare, l'adozione di regolamenti concernenti: l'organizzazione e il funzionamento dell'Agenzia ("Regolamento di organizzazione e funzionamento"); materie di contabilità interna ("Regolamento di contabilità"); procedure per la stipula di contratti di appalti e la fornitura di servizi ("Regolamento sulle procedure per la stipula di contratti di appalti e fornitura di servizi"); e, infine, concernenti il personale ("Regolamento del personale").

[17] Ossia a decorrere dal 5 agosto 2021.

ambito NIS, in conformità a quanto previsto dalle disposizioni del D.Lgs. 65/2018; ii) l'acquisizione di tutte le funzioni in materia di cybersicurezza precedentemente conferite al Ministero dello sviluppo economico (con particolare riferimento ai compiti assegnati al MISE nell'ambito delle disposizioni istitutive del perimetro di sicurezza nazionale cibernetica, del Codice delle comunicazioni elettroniche e, infine, del decreto legislativo di recepimento nazionale della direttiva NIS), nonché tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri e al DIS in ambito perimetro di sicurezza nazionale cibernetica e alle funzioni di cybersicurezza precedentemente destinate all'AgID (riguardo quest'ultima il riferimento, in particolare, è a quanto disposto dall'articolo 51 del decreto legislativo 7 marzo 2005, n. 82 c. d. "Codice dell'amministrazione digitale", rubricato "Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni"). Come anticipato, infine, risultano istituiti presso l'Agenzia anche il Nucleo per la cybersicurezza, il CSIRT Italia e il CVCN.

3. La riorganizzazione del quadro normativo nazionale in materia di cybersicurezza ad opera del D.L. 82/2021 convertito

La seconda direttrice sottesa all'introduzione del D.L. 82/2021 convertito, strettamente correlata alla prima analizzata, attiene alla riorganizzazione del quadro normativo in materia di cybersicurezza nazionale. Sul punto, appare opportuno rammentare sinteticamente gli interventi normativi principali introdotti negli ultimi anni e analizzare come il D.L. 82/2021 convertito sia intervenuto su questi per garantire conformità e attuazione operativa delle disposizioni alla luce del nuovo quadro di *governance* istituzionale di cybersicurezza definito.

L'intervento di modifica prevalente ad opera del D.L.82/2021 convertito, è concentrato sulle disposizioni principali che compongono il quadro normativo nazionale in materia di cybersicurezza, composto, in particolare, dal decreto legislativo 18 maggio 2018, n. 65 (c.d. "decreto legislativo NIS")[18] e dal decreto-legge 21 settembre 2019, n. 105 (c.d. "decreto-legge perimetro")[19].

[18] Decreto legislativo 18 maggio 2018, n. 65 recante "*Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*", disponibile all'indirizzo: www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg.

[19] Decreto-legge 21 settembre 2019, n. 105 recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*" disponibile all'indirizzo: www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg.

Il decreto legislativo NIS stabilisce le misure volte a conseguire un livello elevato di sicurezza complessivo di reti e sistemi informativi in ambito nazionale, contribuendo a incrementare il livello comune di sicurezza dell'Unione europea (articolo 1, comma 1, del decreto legislativo NIS). Destinatari principali delle disposizioni del decreto-legislativo NIS sono gli Operatori dei Servizi Essenziali (c.d. "OSE") e i Fornitori di Servizi Digitali (c.d. "FSD")[20], ai quali sono posti obblighi di introduzione di misure tecniche e organizzative di sicurezza adeguate al rischio e obblighi di notifica in caso di incidente di sicurezza rilevante.
Il quadro definito dal decreto legislativo NIS (precedente all'intervento del D.L. 82/2021 convertito) prevedeva:

- l'istituzione di cinque Autorità nazionali competenti NIS[21], alle quali spettava la responsabilità dell'attuazione delle disposizioni del decreto e l'individuazione degli OSE e a cui erano attribuiti poteri di controllo, ispettivi e sanzionatori;
- la designazione del DIS quale punto di contatto unico[22];
- l'istituzione, presso la Presidenza del Consiglio dei ministri, dello CSIRT italiano per la gestione e risposta tempestiva agli incidenti di sicurezza informatica.

All'interno del quadro descritto, il D.L. 82/2021 convertito modifica nella sostanza quanto previsto dalle disposizioni precedenti del decreto di recepimento della direttiva NIS. Anzitutto, sono suddivise le funzioni destinate all'Autorità nazionale competente NIS da quelle assegnate a un nuovo soggetto: l'Autorità di settore. In sintesi, con le modifiche intervenute di recente a opera del decreto-legge:

- l'Agenzia per la cybersicurezza nazionale diviene unica Autorità nazionale competente NIS, a cui sono attribuiti poteri di controllo, ispettivi e sanzionatori;

[20] Il decreto, in conformità a quanto previsto dalla direttiva NIS, ha recepito i settori coinvolti nell'ambito di applicazione delle disposizioni normative e riportati, nel decreto legislativo di recepimento nazionale, agli Allegati II (per gli OSE) e III (per i FSD).
[21] In particolare, sono state identificate in sede di prima approvazione del decreto legislativo in analisi le seguenti Autorità nazionali competenti NIS: Ministero dell'economia e delle finanze (per i settori bancario e infrastrutture dei mercati finanziari), Ministero dello sviluppo economico (per i settori energia elettrica, gas e infrastrutture digitali), Ministero della salute (per il settore sanitario), Ministero dell'ambiente e della tutela del territorio e del mare (per il settore di fornitura e distribuzione dell'acqua potabile) e Ministero delle infrastrutture e dei trasporti (per il settore trasporti – *e.g.* trasporto aereo).
[22] Organo deputato, ai sensi dell'articolo 3, comma 1, lettera c) del decreto di recepimento, al coordinamento nazionale sui temi di sicurezza delle reti e dei sistemi informativi e alla cooperazione al livello europeo.

- le Autorità di settore[23], di supporto all'Agenzia nell'attuazione delle disposizioni del decreto legislativo NIS, si pongono all'interno del "Comitato tecnico di raccordo" istituito presso l'Agenzia;
- il CSIRT Italia, destinatario delle notifiche in caso di incidente di sicurezza informatica rilevante ai danni di reti e sistemi informativi di OSE e FSD, è istituito, come anticipato, presso l'Agenzia.

Al fianco del decreto legislativo NIS, nel quadro normativo di cybersicurezza nazionale, si pone il decreto-legge perimetro, di istituzione del Perimetro di Sicurezza Nazionale Cibernetica (di seguito anche "PSNC" o "Perimetro"), introdotto al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici (c.d. "Beni ICT") di operatori pubblici e privati, necessari allo svolgimento di funzioni essenziali per lo Stato ovvero necessari alla prestazione di servizi essenziali, dalla cui compromissione possa derivare un pregiudizio alla sicurezza nazionale[24].

In tale prospettiva, il decreto-legge perimetro (le cui disposizioni sono dettagliate da ulteriori provvedimenti attuativi) prevede l'individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati (aventi una sede nel territorio nazionale) e tenuti al rispetto delle misure e degli obblighi previsti dalle disposizioni del decreto-legge medesimo[25] e, in particolare, obbligati a: i) redigere e aggiornare l'elenco dei Beni ICT rientranti nel Perimetro; ii) adottare misure volte a garantire elevati livelli di sicurezza dei Beni ICT e

[23] In particolare, nella nuova definizione di ruoli e responsabilità, le Autorità di settore possono proporre all'Agenzia eventuali variazioni all'elenco degli OSE e, più in generale, collaborano con l'Agenzia nell'attuazione delle disposizioni del decreto legislativo NIS. Le Autorità di settore attualmente identificate sono: il Ministero dello sviluppo economico (per il settore infrastrutture digitali), il Ministero delle infrastrutture e della mobilità sostenibili (per il settore trasporti), il Ministero dell'economia e delle finanze (per il settore bancario e delle infrastrutture dei mercati finanziari), il Ministero della salute (per le attività di assistenza sanitaria), il Ministero della transizione ecologica (per il settore energia), coadiuvato, per alcuni settori, dalle Regioni e Province autonome di Trento e Bolzano (in particolare, per il settore fornitura e distribuzione dell'acqua potabile). Si veda, in tal senso, quanto disposto dall'articolo 15, comma 1, lettera g) del D.L. 82/2021 convertito.

[24] Risulta opportuno rammentare in tale sede che il decreto-legge perimetro prevede, per ciascun ambito principale di intervento (*e.g.* adozione di misure di sicurezza e notifica in caso di incidente di sicurezza), l'adozione di regolamenti attuativi di rango secondario, essenziali per l'operatività effettiva delle disposizioni del decreto-legge.

[25] Il D.P.C.M. 30 luglio 2020, n. 131 in attuazione di quanto previsto dall'articolo 1, comma 2, del decreto-legge perimetro, disciplina i criteri per l'identificazione dei Soggetti, pubblici e privati, da includere nel PSNC, nonché per la predisposizione, l'aggiornamento e la trasmissione degli elenchi di servizi, sistemi e reti a supporto delle funzioni essenziali individuate. Il testo del decreto è disponibile all'indirizzo: www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg.

notificare gli incidenti di sicurezza aventi impatto sui Beni ICT[26]; iii) infine, notificare al CVCN la volontà di procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sui Beni ICT[27].
All'interno del quadro descritto, il D.L. 82/2021 convertito interviene modificando diverse disposizioni del decreto-legge perimetro. Anzitutto, in coerenza con la nuova architettura di governance, l'Agenzia acquisisce tutti i compiti e le funzioni precedentemente attribuiti alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico (quali, a titolo esemplificativo, la stesura dell'elenco di misure tecniche e organizzative di sicurezza che i soggetti rientranti nel Perimetro devono adottare). Le notifiche degli incidenti di sicurezza sui Beni ICT sono da inoltrare al CSIRT Italia (istituito presso l'Agenzia), mentre le notifiche circa la volontà di acquisire beni e servizi da impiegare sui Beni ICT, sono da effettuare al CVCN (anch'esso istituito presso l'Agenzia)[28]. Tutti i riferimenti al DIS sono ora sostituiti con i richiami all'Agenzia; al contempo, i riferimenti al CISR sono sostituiti con rimandi al CIC.

4. Conclusioni

Il D.L. 82/2021 convertito ha, in definitiva, completamente riformato l'architettura istituzionale di cybersicurezza, riorganizzando ruoli e responsabilità specifiche e il quadro normativo di riferimento, ponendo al centro della nuova governance l'Agenzia per la cybersicurezza nazionale.
La straordinaria necessità e urgenza sottesa all'introduzione del decreto-legge in analisi, dettata dal numero esponenziale di attacchi e incidenti di cyber-

[26] Il D.P.C.M. 14 aprile 2021, n. 81 definisce le procedure, i termini e le modalità di notifica degli incidenti di sicurezza allo CSIRT italiano, nonché le misure minime di sicurezza da applicare a servizi, sistemi e reti a supporto delle funzioni essenziali individuate. Il testo del decreto è disponibile all'indirizzo: www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg.
[27] Su tale punto, si rileva l'approvazione di due provvedimenti: a) il D.P.R. 5 febbraio 2021, n. 54 che definisce procedure, modalità e termini da seguire per l'affidamento a fornitori esterni di beni e servizi ICT e con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti dal Decreto-legge n. 105 del 2019, disponibile all'indirizzo www.gazzettaufficiale.it/eli/id/2021/04/23/21G00060/sg ; e, b) il D.P.C.M. 15 giugno 2021 che definisce le categorie di beni e servizi, destinati a essere impiegati sulle reti e sui sistemi a supporto delle Funzioni Essenziali, per cui i Soggetti inclusi nel PSNC sono tenuti a comunicare al CVCN l'eventuale affidamento a fornitori esterni. Il testo del decreto è disponibile all'indirizzo www.gazzettaufficiale.it/eli/id/2021/08/19/21A05087/sg.
[28] L'articolo 16, comma 9, lettera a) del decreto-legge n. 82/2021 convertito, prevede che l'obbligo di comunicazione al CVCN sarà efficace a decorrere dal trentesimo giorno successivo alla pubblicazione del D.P.C.M. che attesterà l'operatività del CVCN e, in ogni caso, a partire dal 30 giugno 2022.

sicurezza, è anche strettamente correlata all'attuazione del PNRR, in cui la sicurezza dello spazio cibernetico rappresenterà un ruolo fondamentale nel garantire l'effettiva ripresa sociale ed economica del Paese, costituendone il volàno principale. Non a caso, tra le milestones del cronoprogramma attuativo degli interventi previsti dal PNRR in ambito di cybersicurezza, era prevista l'istituzione dell'Agenzia e l'adozione del relativo regolamento interno tramite D.P.C.M., entro il terzo quarter del 2022.

Sempre dall'analisi delle milestones del cronoprogramma emerge, inoltre, come l'istituzione dell'Agenzia rappresenti solamente un punto di partenza nello sviluppo delle capacità di resilienza nazionali; è probabile, inoltre, che la stessa architettura istituzionale (appena ridefinita) possa essere ulteriormente aggiornata e ampliata nel breve-medio termine. È infatti previsto (sempre entro il termine, intermedio, del terzo quarter del 2022, con ulteriore verifica di attuazione completa nel 2024[29]) che all'interno dell'architettura istituzionale di cybersicurezza siano innestatati anche un centro nazionale di condivisione e analisi delle informazioni ("ISAC"), un HyperSOC nazionale e il centro di calcolo ad alte prestazioni integrato dagli strumenti di intelligenza artificiale/apprendimento automatico (AI/ML) per l'analisi degli incidenti di cybersicurezza di portata nazionale, con annessa istituzione, presso l'Agenzia, di un'unità centrale di audit per quanto attiene l'adozione delle misure di sicurezza NIS e PSNC. Il quadro di governance di cybersicurezza nazionale, dunque, è in continua definizione e aggiornamento, in coerenza con le caratteristiche intrinseche del mondo digitale e dell'evoluzione delle relative minacce alla sua sicurezza.

In tale contesto soggetto a rapidi cambiamenti, il D.L. 82/2021 convertito si pone, in definitiva, come intervento necessario per garantire la resilienza cibernetica nazionale, anche in ottica propedeutica al rilancio economico-sociale post-pandemico, di cui rappresenta perno fondamentale: l'efficace realizzazione della ripresa nazionale è, infatti, strettamente correlata allo sviluppo di capacità e competenze adeguate atte a garantire la sicurezza dello spazio cibernetico. Lo sviluppo del mercato digitale, volàno per la ripresa, è subordinato alla garanzia di affidabilità di reti e sistemi informativi e, più in generale, della sicurezza delle infrastrutture digitali a esso strumentali.

La speranza è che l'istituzione del complesso e articolato ecosistema, così come rappresentato nel corso della trattazione, non resti un esercizio di stile

[29] Sul punto si veda il *dossier* redatto dal Servizio Studi della Camera dei Deputati e del Senato della Repubblica "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", disponibile all'indirizzo: https://www.senato.it/service/PDF/PDFServer/BGT/01306371.pdf.

teso esclusivamente a coprire una serie di mancanze che sono state notate all'interno dell'architettura nazionale in termini di contrasto al rischio cyber, ma costituisca un effettivo punto di svolta. Ciò che si auspica è un'efficace messa a regime dell'Agenzia che aiuti il Paese a gestire il rischio per cui se l'Agenzia stessa non venisse correttamente indirizzata potrebbe trasformarsi in un macigno istituzionale con poche leve per agire in modo concreto, vista la pletora di entità che è chiamata a coordinare e con cui è comandata di collaborare.

Il tempismo con cui il decreto è stato convertito in legge proprio nei giorni in cui l'attacco alla Regione Lazio[30] è balzato agli onori delle cronache alimenta qualche perplessità che speriamo siano fugate nel corso dei mesi a venire.

[30] Si veda a tal proposito di V. Balocco, *Regione Lazio sotto attacco hacker, Zingaretti: "Azione terroristica"*, in *corrierecomunicazioni.it*, 2 agosto 2021, disponibile all'indirizzo: https://www.corrierecomunicazioni.it/cyber-security/regione-lazio-sotto-attacco-hacker-zingaretti-azione-terroristica/.