*La Comunicazione - Note, Recensioni e Notizie n. 67*
***Anno 2023***

# La nuova architettura di cybersicurezza in Italia

## *Italy's new cybersecurity institutional architecture*

Claudia Meloni♦[1]

♦ Agenzia per la cybersicurezza nazionale

**Sommario**

Il decreto-legge 14 giugno 2021, n. 82, ha disposto una complessiva riforma dell'architettura istituzionale in materia di cybersicurezza, operando un riordino e una razionalizzazione delle competenze attribuite ai diversi attori istituzionali. In particolare, è stato istituito un nuovo ente pubblico, l'Agenzia per la cybersicurezza nazionale, incaricato di tutelare gli interessi nazionali nel campo della cybersicurezza. Dopo quasi due anni dall'emanazione del decreto-legge n. 82/2021, in questo articolo si intende fornire una breve ricostruzione del nuovo assetto normativo e di come lo stesso sia stato attuato da un punto di vista ordinamentale con il fine ultimo di innalzare i livelli complessivi di cybersicurezza del Paese.

**Abstract**

The Law Decree no. 82 of June 14th, 2021, has provided for a general reform of the cybersecurity institutional architecture, by reorganizing and rationalizing the various institutional actors' competences. In particular, a new public entity has been established, the National Cybersecurity Agency, which is responsible for the protection of national interests in the cybersecurity field. After nearly two years from issuing the law decree no. 82/2021, this article intends to provide a short description of the new regulatory structure and of how this has been implemented with the ultimate aim of increasing the general cybersecurity level of the Country.

---

[1] Le opinioni espresse nel presente lavoro sono riconducibili esclusivamente all'autrice e non impegnano in alcun modo l'Amministrazione di appartenenza.

**Keyword**

Cybersecurity. Italian National Cybersecurity Agency. Italian cybersecurity institutional structure. Institutional reform.

## 1 - Introduzione

"*La cybersecurity è un problema complesso per il quale sono necessarie soluzioni efficaci e coordinate*"[2]. Quest'ineludibile complessità dello spazio cibernetico deriva dal fatto che il mondo digitale è colmo, oltre che di innumerevoli opportunità, anche di altrettanti rischi. Infatti, come dichiarato nella Strategia nazionale di cybersicurezza 2022-2026, adottata dal Presidente del Consiglio dei ministri il 17 maggio 2022, "*i rischi insiti in tale complessità – e le potenziali, molteplici ricadute negli ambiti economico, sociale e politico – spaziano dalla dipendenza tecnologica e perdita di autonomia strategica dello Stato alle minacce di tipo antropico, in cui l'errore umano si somma alle iniziative di attori malevoli, caratterizzati da diverso grado di sofisticazione e mossi da differenti, ma ugualmente dannosi, intenti*"[3].

Oltre ai molteplici fattori di rischio, la complessità è accresciuta dal fatto che lo spazio cibernetico è per sua natura trasversale, dato che gran parte delle attività ivi svolte sono funzionali allo svolgimento di funzioni o servizi essenziali attinenti ai più diversi settori della società come, ad esempio, quello sanitario, delle telecomunicazioni, dei trasporti ed energetico[4].

[2] OA – Osservatorio ACCREDIA, "Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata", p. 1, 1, 2022.

[3] Strategia nazionale di cybersicurezza 2022-2026, p. 4.

[4] Si faccia riferimento, a titolo esemplificativo, ai numerosi settori inclusi nell'Allegato I della nuova 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, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

Infatti, sull'onda del processo di trasformazione digitale della società e della pubblica amministrazione[5], la fornitura dei suddetti servizi si avvale in gran parte dell'utilizzo di sistemi, servizi e infrastrutture digitali[6] (c.d. beni ICT). Di conseguenza, eventuali incidenti che compromettono il funzionamento dei beni ICT utilizzati per lo svolgimento di tali funzioni e/o servizi possono pregiudicare la possibilità, da un lato, della collettività di avere a disposizione quest'ampia varietà di prestazioni, dall'altro, dell'individuo di godere di alcuni diritti fondamentali, costituzionalmente riconosciuti, strettamente correlati alla fruizione di servizi essenziali. In poche parole, si può dire che "la cybersicurezza riguarda tutti"[7].

Proprio in ragione della complessità dello spazio cibernetico, vi sono molteplici interessi da tutelare e attori chiamati ad assolvervi i propri compiti istituzionali.

Il Governo aveva agito, fin dal 2013, per stabilire un quadro normativo che disciplinasse la tematica della protezione cibernetica del Paese, a partire dalle infrastrutture critiche materiali e immateriali, adottando il dPCM del 24 gennaio 2013 "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*". Questo decreto era stato poi sostituito dal dPCM 17 febbraio 2017, che aveva riformato l'assetto istituzionale definito nel 2013. Al contempo, avevano iniziato a susseguirsi una serie di atti normativi di rango primario

[5] Boschetti B., "La transizione della pubblica amministrazione", in Lalli A. (a cura di) *L'amministrazione pubblica nell'era digitale*, pp. 1- 44, 2022.

[6] Montagnani E., "Le pubbliche amministrazioni nell'era delle tecnologie cloud ed edge computing tra opportunità e rischi: il Piano nazionale di ripresa e resilienza e le comunità digitali", in L. Abba, A. Lazzaroni e M. Pietrangelo (a cura di), *La internet governance e le sfide della trasformazione digitale*, pp. 251-266, 2022.

[7] Vedi discorso del Pref. Bruno Frattasi, Direttore generale dell'ACN https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-frattasi-in-italia-troppi-attacchi-sommersi/

che avevano disciplinato in maniera "settoriale"[8] la tutela del Paese nello spazio cibernetico, andando chiaramente ad incidere anche sull'assetto istituzionale[9].

Tuttavia, sebbene il Paese avesse profuso notevole impegno nel definire normativamente specifici obblighi per gli operatori pubblici e privati del settore della cybersicurezza – innalzando, in tal modo, il livello di cybersicurezza del Paese (con particolare attenzione ai settori critici per la società) –, a questo susseguirsi di norme settoriali non era corrisposto un parallelo e complessivo ripensamento del riparto delle competenze. Piuttosto, ciascun nuovo atto normativo assegnava la nuova funzione allo specifico ente che sembrasse, di volta in volta, più appropriato *rationae materiae*. Ciò aveva comportato una frammentarietà delle competenze istituzionali, con un corrispondente quadro normativo composito e stratificato[10].

Uno dei casi più esemplificativi di questo concetto è l'assetto organizzativo derivante dal recepimento della direttiva (UE) 2016/1148, c.d. "direttiva NIS". Infatti, il d. lgs. n. 65/2018 aveva originariamente previsto, invece che una singola Autorità nazionale competente NIS, tante autorità competenti quanti sono i diversi settori compresi nella direttiva[11]. Tra questi sono ricompresi anche quello sanitario e della distribuzione di acqua potabile, per i quali il

[8] Con il termine "settoriale" si vuole intendere la disciplina di specifici ambiti della cybersicurezza, come ad esempio: il Regolamento (UE) 2019/881 (c.d. Cybersecurity Act), che interviene in materia di certificazione; il decreto-legge 21 settembre 2019, n. 105, (c.d. decreto-legge perimetro), che stabilisce obblighi per quei soli settori, soggetti e beni ICT inclusi nel Perimetro di sicurezza nazionale cibernetica; il decreto legislativo n. 259/2003, codice delle comunicazioni elettroniche, che dispone in materia di misure di sicurezza e notifiche di incidenti che impattavano reti di comunicazione elettronica. Tra questi atti normativi è ricompreso anche il decreto legislativo 18 maggio 2018, n. 65, di attuazione della 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, che quale primo atto normativo di rango primario in materia, aveva disposto una disciplina complessiva in materia di misure di sicurezza e obbligo di notifica degli incidenti.

[9] Renzi A., "La sicurezza cibernetica: lo stato dell'arte", in *Giornale Dir. Amm.*, p. 538, 2021, 4.

[10] Parona L., "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale Dir. Amm.*, p. 709, 2021, 6.

[11] Art. 7 del d. lgs. n. 65/2018.

ruolo di Autorità NIS era condiviso tra, rispettivamente, il Ministero della salute e le Regioni e Province Autonome e il Ministero dell'ambiente e della sicurezza energetica e le Regioni e Province Autonome. Facendo il calcolo, si arriva a più di 20 Autorità competenti, ciascuna con poteri regolamentari, ispettivi e sanzionatori.

Alla luce di questa stratificazione normativa[12], nonché dell'esigenza di approcciare la materia secondo una dimensione olistica[13], la necessità di ridefinire l'attribuzione di competenze era da tempo avvertita. Nel 2021 si è quindi arrivati ad una rinnovata architettura istituzionale, che ha previsto la creazione di una nuova Autorità nazionale competente in materia, l'Agenzia per la cybersicurezza nazionale (ACN).

Nei successivi paragrafi si intende fornire una breve ricostruzione del nuovo assetto normativo e di come lo stesso sia stato attuato da un punto di vista ordinamentale con il fine di innalzare i livelli complessivi di cybersicurezza del Paese.

## 2 – Il quadro di *governance*

La riforma operata dal d.l. n. 82/2021 ha determinato una riorganizzazione delle competenze a livello nazionale, istituendo nuovi attori istituzionali, razionalizzando e armonizzando l'esercizio delle relative funzioni. Ciò creando un sistema sinergico, al quale partecipano le amministrazioni pubbliche, l'accademia, gli enti di ricerca e il settore privato, che concorrono a salvaguardare la cybersicurezza nazionale.

Questa scelta soddisfa non solo l'esigenza di unitarietà, ma anche la necessità di approcciare tale problematica secondo una dimensione olistica, nella quale la tematica della cybersicurezza venga affrontata da un punto di vista, oltre che prettamente "tecnico" – con

[12] Parona L., "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale Dir. Amm.*, p. 709, 2021,6.

[13] Relazione illustrativa al d.d.l. "*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'Agenzia per la cybersicurezza nazionale*", p. 2.

obblighi di adozione delle misure di sicurezza e segnalazione degli incidenti cyber –, anche "sociale", cioè investendo sulla formazione, sullo sviluppo tecnologico nazionale e sulla cultura della cybersicurezza.

Questi ambiti, infatti, sono imprescindibili per garantire un elevato livello di cybersicurezza del Paese, considerato che le sole soluzioni tecniche, senza la disponibilità di personale adeguatamente formato per implementare le relative misure e gestire gli incidenti ovvero di utenti consapevoli delle minime azioni di "*cyber hygiene*" da adottare, non sono sufficienti a diminuire il rischio *cyber*.

### 2.1 L'organizzazione istituzionale precedente alla riforma del d.l. n. 82/2021

Prima di illustrare la riforma, risulta certamente utile fornire una sommaria descrizione dell'assetto precedente. Da un punto di vista normativo, il principale testo di riferimento era il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*", che definiva 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[14].

Secondo tale struttura, il vertice politico era il Presidente del Consiglio dei ministri, che determinava le politiche e gli indirizzi in materia, adottando gli atti di indirizzo strategico quali il Quadro strategico nazionale per la sicurezza dello spazio cibernetico, il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali[15].

[14] Peluso F., "La disciplina italiana in tema di cybersecurity", in Contaldo A., Mula D. (a cura di) *Cybersecurity Law, Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche,* pp. 120-147, 2020.

[15] Renzi A., "La sicurezza cibernetica: lo stato dell'arte", in *Giornale Dir. Amm.*, p. 538, 2021, 4.

Sempre a livello politico, il Presidente del Consiglio dei ministri era affiancato dal Comitato interministeriale per la sicurezza della Repubblica (CISR) che, relativamente alla materia della sicurezza nello spazio cibernetico, esercitava diverse funzioni di consulenza, di proposta e deliberative.

A livello operativo-tecnico, le competenze in materia di cybersicurezza erano ripartite tra una molteplicità di attori istituzionali, sulla base delle specifiche funzioni ad essi attribuite dagli atti normativi di settore[16]. Tra i principali possono individuarsi, oltre alle già citate Autorità competenti NIS[17], la Presidenza del Consiglio dei ministri, in particolare il Dipartimento per la trasformazione digitale (DTD), il Dipartimento delle informazioni per la sicurezza (DIS), il Ministero delle imprese e del made in Italy (MIMIT) e l'Agenzia per l'Italia digitale (AgID).

Ad esempio, con riferimento al Perimetro di sicurezza nazionale cibernetica, il supporto al Presidente del Consiglio dei ministri nell'attuazione coordinata della normativa in materia era affidato al DIS[18], il cui Vice Direttore generale presiedeva anche il Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica[19]. Le relative funzioni ispettive e sanzionatorie erano, invece, ripartite tra il Dipartimento per la trasformazione digitale, per i soggetti pubblici, e il Ministero delle imprese e del made in Italy, per i soggetti privati.

Presso il Dipartimento delle informazioni per la sicurezza era anche costituito il CSIRT italiano[20], destinatario di tutte le notifiche di incidente cibernetico.

---

[16] Vedi nota 7.

[17] Vedi Introduzione.

[18] Art. 1, comma 19-bis, del decreto-legge n. 105/2019.

[19] Art. 6 del dPCM n. 131/2020 "*Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*".

[20] dPCM 8 agosto 2019 "*Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT Italia*".

In ambito di certificazione della cybersicurezza, le competenze erano prevalentemente esercitate dal Ministero delle imprese e del made in Italy, che era anche amministrazione competente in materia di sicurezza delle comunicazioni elettroniche, il cui Istituto superiore delle comunicazioni e delle tecnologie dell'informazione era destinatario, insieme al CSIRT, delle relative notifiche di incidente[21].

Ancora su un altro ambito, quello della determinazione dei livelli minimi di sicurezza della futura infrastruttura del c.d. *cloud* nazionale[22], nonché delle linee guida per la sicurezza dei sistemi e delle infrastrutture digitali della P.A., le funzioni erano esercitate dall'Agenzia per l'Italia digitale[23].

Da questa illustrazione, sebbene sintetica, si può percepire come nell'assetto previgente mancasse una "gestione" unitaria della cybersicurezza, con conseguenti difficoltà sia nel definire un approccio uniforme all'attuazione degli obblighi in materia, anche in termini di indirizzo dei soggetti vigilati, sia nell'avere una visione a tutto tondo dello stato della cybersicurezza.

### 2.2 La nuova struttura istituzionale

La riforma operata dal decreto-legge n. 82/2021 è, dunque, intervenuta proprio per porre un rimedio alle suddette problematiche e strutturare un ecosistema nazionale nel quale fosse presente un singolo ente incaricato del coordinamento della materia della cybersicurezza, sotto l'indirizzo del vertice politico.

Nella nuova architettura, il vertice politico è rimasto il Presidente del Consiglio dei ministri, che ha l'alta direzione e la responsabilità generale delle politiche di cybersicurezza. Tra gli altri

[21] Decreto 12 dicembre 2018 del Ministero dello sviluppo economico recante "*Misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi*".

[22] Art. 33-septies del d.l. 18 ottobre 2012, n. 179, recante "*Ulteriori misure urgenti per la crescita del Paese*".

[23] Artt. 51 e 71 del decreto legislativo 7 marzo 2005, n. 82, recante "*Codice dell'amministrazione digitale*".

poteri del Presidente del Consiglio dei ministri rientrano l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza, la nomina e la revoca del Direttore generale e del Vice Direttore generale dell'Agenzia per la cybersicurezza nazionale, previa deliberazione del Consiglio dei ministri, nonché quello di impartire le direttive per la cybersicurezza ed emanare ogni disposizione necessaria per l'organizzazione e il funzionamento dell'ACN[24].

La normativa prevede, inoltre, che il Presidente del Consiglio dei ministri possa delegare l'esercizio dei poteri non attribuiti in via esclusiva all'Autorità delegata per la sicurezza della Repubblica di cui all'articolo 3 della legge 124/2007[25].

Il Presidente del Consiglio dei ministri e l'Autorità delegata rappresentano, dunque, le autorità politiche d'indirizzo e di riferimento per le attività dell'Agenzia, in continuità con la scelta già fatta al tempo con il menzionato dPCM del 17 febbraio 2017.

Sempre in continuità, ma con un significativo elemento di innovazione, è stata mantenuta la scelta di far affiancare il Vertice politico da un consesso interministeriale che potesse coadiuvarlo nella determinazione degli indirizzi generali di cybersicurezza e nell'alto coordinamento delle politiche in materia.

A tal fine, è stato istituito, presso la Presidenza del Consiglio dei ministri, il Comitato interministeriale per la cybersicurezza (CIC), che ha assunto le funzioni in materia previamente esercitate dal CISR[26]. Esso è istituito con funzioni di consulenza, proposta e vigilanza e rappresenta la sede politica nella quale esaminare e indirizzare le problematiche relative alla cybersicurezza, condividere gli obiettivi strategici e gli indirizzi, nonché monitorare

[24] Art. 2 del decreto-legge n. 82/2021.

[25] Art. 3 del decreto-legge n. 82/2021.

[26] Ad eccezione di quelle previste dall'articolo 5 del decreto-legge n. 105/2019.

l'attuazione delle politiche in materia[27]. E, infatti, il decreto-legge n. 82/2021 prevede anche che l'esercizio del citato potere del Presidente del Consiglio dei ministri di impartire le direttive in materia contempli il coinvolgimento del CIC.

Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro delle imprese e del made in Italy, dal Ministro dell'ambiente e della sicurezza energetica, dal Ministro dell'università e della ricerca, dal Ministro delle infrastrutture e dei trasporti e dal Ministro delegato per l'innovazione tecnologica e la transizione digitale (non presente nell'attuale compagine governativa, in quanto non nominato).

Tra i poteri del CIC rientra quello di proporre al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza e promuovere l'adozione delle iniziative necessarie a favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati, la condivisione delle informazioni, l'adozione di migliori pratiche e di misure per lo sviluppo industriale, tecnologico e scientifico. In maniera complementare al citato potere di proposta, il CIC esercita l'alta sorveglianza sull'attuazione della Strategia nazionale di cybersicurezza, che consente certamente sia una verifica collegiale e condivisa dello stato della cybersicurezza del Paese, sia l'identificazione di eventuali *gap* esistenti e ambiti verso i quali indirizzare le politiche di governo in materia. Oltre a queste di ampio respiro, il CIC esercita anche alcune funzioni più mirate sulle attività dell'Agenzia per la cybersicurezza nazionale, esprimendo parere sull'adozione dei dPCM che ne disciplinano, tra l'altro, l'organizzazione e il funzionamento, nonché il rapporto di lavoro alle dipendenze dell'ente. Il CIC esprime, inoltre, parere sull'approvazione dei bilanci preventivo e consuntivo.

[27] Art. 4 del d.l. n. 82/2021.

Considerata la trasversalità degli interessi nel cyberspazio, pur avendo voluto accentrare le competenze in una struttura unitaria, la riforma non ha impattato le importanti funzioni in materia di: *cyber-intelligence*[28], già di competenza degli organismi di informazione per la sicurezza; *cyber-defense*, già di competenza del Ministero della difesa; prevenzione e repressione dei reati, già di competenza delle Forze di polizia. Al contempo, con queste è garantito un coordinamento negli altri consessi interistituzionali che saranno analizzati nel prosieguo, sempre per assicurare una visione complessiva dello stato della cybersicurezza.

## 3 – L'Agenzia per la cybersicurezza nazionale

Nell'ambito della rinnovata architettura nazionale, l'elemento sicuramente più innovativo è stata la creazione di un nuovo ente, istituito *ad hoc* per la tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Si tratta dell'ACN, che assume il ruolo di Autorità nazionale in materia, accentrante la gran parte delle funzioni e incaricata del coordinamento dei soggetti pubblici coinvolti nella cybersicurezza, anche al fine di assicurare l'unicità istituzionale di indirizzo e di azione.

### 3.1 L'assetto istituzionale dell'ACN

L'Agenzia è un ente pubblico con personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. Essa opera a supporto del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, per l'esercizio delle competenze attribuite dal decreto-legge n. 82/2021[29].

[28] Sulla definizione di cyber-intelligence, vedi Bonfanti M.E., "Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice", *INSS Cyber, Intelligence, and Security*, pp. 105-121, Vol. 2, No. 1, 2018.

[29] Art. 5 del d.l. n. 82/2021.

L'assetto istituzionale dell'ACN risulta d'interesse in quanto, pur essendo un'agenzia governativa che risponde del proprio operato al Vertice dell'Esecutivo, essa non è governata dalla tradizionale disciplina stabilita nel d. lgs. n. 300/1999[30] ma presenta una sua peculiare struttura. L'ordinamento dell'ACN è, infatti, definito nel decreto-legge n. 82/2021 e nei relativi regolamenti di attuazione, adottati con decreto del Presidente del Consiglio dei ministri. Questi ultimi sono, precisamente: 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 (dPCM 1 settembre 2022, n. 166).

Essa si configurerebbe, dunque, come un "*tertium genus*", in quanto il particolare modello organizzativo adottato – che prende ispirazione anche da quello della Banca d'Italia, in attuazione di quanto disposto dall'articolo 12, comma 1, del d.l. n. 82/2021[31] – non è assimilabile a quello previsto per le altre analoghe agenzie.

Questa innovativa struttura istituzionale è stata ritenuta necessaria dal Legislatore per consentire all'Agenzia di esercitare nel modo più efficace e adeguato le rilevanti funzioni di tutela della sicurezza nazionale ad essa attribuite e, infatti, nella relazione illustrativa del

[30] Parona L., "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale Dir. Amm.*, p. 709, 2021, 6.

[31] Art. 12, comma 1, d.l. n. 82/2021 "1*. Con apposito regolamento è dettata, nel rispetto dei principi generali dell'ordinamento giuridico, anche in deroga alle vigenti disposizioni di legge, ivi incluso il decreto legislativo 30 marzo 2001, n. 165, e nel rispetto dei criteri di cui al presente decreto, la disciplina del contingente di personale addetto all'Agenzia, tenuto conto delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia. Il regolamento definisce l'ordinamento e il reclutamento del personale, e il relativo trattamento economico e previdenziale, prevedendo, in particolare, per il personale dell'Agenzia di cui al comma 2, lettera a), un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia, sulla scorta della equiparabilità delle funzioni svolte e del livello di responsabilità rivestito.*"

decreto-legge, è ben spiegato come "*la particolarità dell'ambito di attività nel quale sarà chiamata ad operare l'istituenda Agenzia – e cioè quello della tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico – e le interazioni che necessariamente avrà con il Sistema di informazione per la sicurezza della Repubblica, hanno portato a definire una disciplina speciale, con l'individuazione degli opportuni punti di equilibrio, attribuendo all'Agenzia una configurazione giuridica che non segue il modello delle agenzie di cui al decreto legislativo 30 luglio 1999, n. 300, quanto piuttosto quello definito dalla legge n. 124 del 2007 per il DIS, AISE e AISI, al quale sono stati apportati i necessari adattamenti conseguenti alla non appartenenza al Comparto intelligence*"[32].

A conferma di quest'impostazione, è stato previsto che il Comitato parlamentare per la sicurezza della Repubblica (COPASIR) – lo stesso Comitato che vigila sull'attività del Sistema di informazione per la sicurezza della Repubblica – eserciti uno specifico controllo sulle attività svolte dall'Agenzia a tutela della sicurezza nazionale. Difatti, il COPASIR è destinatario di un insieme di comunicazioni informative da parte dell'ACN, tra cui la Relazione annuale sulle attività svolte a tutela della sicurezza nazionale di cui all'articolo 14, comma 2, del d.l. n. 82/2021. Inoltre, il Comitato esprime parere su tutti e quattro i regolamenti che disciplinano l'ordinamento e il funzionamento dell'Agenzia e può udirne il Direttore generale[33].

La struttura organizzativa è delineata dall'articolo 6 del d.l. n. 82/2021, che ne prevede l'articolazione fino ad un numero massimo di otto uffici di livello dirigenziale generale, nonché fino ad un numero massimo di trenta articolazioni di livello dirigenziale non generale. Lo stesso individua, inoltre, come organi dell'Agenzia, il Direttore generale (che è il diretto referente del

[32] Relazione illustrativa al d.d.l. "*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'Agenzia per la cybersicurezza nazionale*", p. 5.

[33] Art. 5 del d.l. n. 82/2021.

Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita) e il Collegio dei revisori dei conti e prevede la figura del Vice Direttore generale. A quest'ultimo è stato attribuito, con il dPCM n. 223/2021, il ruolo di coadiuvare il Direttore generale nella direzione dell'ente e/o sostituirlo nei casi di assenza o impedimento. Sulla base di apposito provvedimento del Direttore generale, può inoltre 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[34].

Anche la composizione dell'organo di controllo è stata definita nel medesimo dPCM che, all'articolo 7, prevede che il Collegio dei revisori dei conti è composto da tre componenti effettivi e uno supplente, di cui: un magistrato della Corte dei conti, in servizio o in quiescenza, che lo presiede; un componente effettivo, designato dal Ministero dell'economia e delle finanze ai sensi dell'articolo 16 della legge 31 dicembre 2009, n. 196; 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[35].

La struttura di dettaglio dell'ACN è stata anch'essa definita dal già citato dPCM n. 223/2021, che ne prevede l'articolazione in Servizi, nel numero di sette, e Divisioni e contempla la possibilità di istituire gruppi di progetto, nonché strutture di missione temporanea di livello dirigenziale o unità di progetto non aventi natura dirigenziale, dedicate all'attuazione di un progetto di durata definita.

[34] Art. 6 del dPCM n. 223/2021.

[35] Art. 7 del dPCM n. 223/2021.

In particolare, i Servizi che sono stati individuati sono: il Gabinetto, che svolge attività di coordinamento e assicura il supporto al Vertice; Autorità e sanzioni, che svolge le funzioni di regolamentazione e la connessa attività sanzionatoria; Certificazione e vigilanza, che sovrintende ai processi di certificazione, qualificazione e valutazione, nonché cura l'attività ispettiva e di verifica; Operazioni, che svolge le funzioni di preparazione, prevenzione, gestione e risposta a eventi cibernetici; Programmi industriali, tecnologici, di ricerca e formazione, che svolge funzioni di indirizzo e gestione delle attività svolte dall'Agenzia per promuovere l'autonomia strategica e la sovranità tecnologica nazionale; Risorse umane e strumentali, che svolge le funzioni connesse alla gestione del personale e dell'attività amministrativa; Strategie e cooperazione, che definisce gli indirizzi strategici e gli strumenti di policy nazionali in materia di cybersicurezza, ne monitora l'attuazione, nonché mantiene e sviluppa le relazioni e la cooperazione internazionale[36].

### 3.2 Le funzioni dell'ACN

Conformemente "*all'approccio olistico*" che ha guidato la riforma, all'Agenzia sono state attribuite – *ex novo* o a seguito di trasferimento da altre Amministrazioni – le più diverse funzioni per la tutela degli interessi nazionali nello spazio cibernetico, partendo dall'attività di prevenzione e gestione degli attacchi *cyber* fino allo sviluppo tecnologico del Paese, passando per la promozione della formazione, lo sviluppo di una forza lavoro specializzata in materia, l'incremento della consapevolezza *cyber*, la cooperazione internazionale e la certificazione dei prodotti ICT.

Proprio in virtù di questa varietà, si può comprendere come l'Agenzia rappresenti il punto di raccordo del quale si era ravvisata la necessità, in grado di avere una percezione complessiva dello stato della cybersicurezza del Paese e di individuare i *gap* ai quali sia necessario porre rimedio attraverso misure adeguate, come, ad esempio, interventi normativi mirati, sviluppo

[36] Art. 12 del dPCM n. 223/2021.

di progettualità, potenziamento della capacità *cyber* della P.A. o una capillare rete di monitoraggio degli incidenti.

Questo fine è ben chiaro anche alla luce del dettato letterale dell'articolo 7 del d.l. n. 82/2021 che, nell'elencare le funzioni dell'ACN, individua, tra le prime, quella 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*"[37].

Questa molteplicità di funzioni determina che l'Agenzia assuma anche diversi "ruoli", a seconda dell'atto normativo settoriale di riferimento, con connessi poteri regolamentari, ispettivi e sanzionatori.

Ad esempio, un ruolo è quello di Autorità nazionale di certificazione della cybersicurezza riferibile, in senso stretto, ai compiti derivanti dal *Cybersecurity Act*, ma al quale possono essere relazionate, in senso lato, anche le attività come Organismo di certificazione della sicurezza informatica (OCSI). Sempre su questo tema, ma nell'ambito del Perimetro di sicurezza nazionale cibernetica (PSNC), è istituito presso l'ACN il Centro di valutazione e certificazione nazionale (CVCN), che svolge lo scrutinio tecnologico in relazione ai beni, sistemi e servizi ICT destinati ad essere impiegati sui beni ICT inseriti nel PSNC.

Un altro ruolo è quello di Autorità nazionale competente e punto di contatto unico NIS, ai sensi del quale, ad esempio, identifica gli operatori dei servizi essenziali e individua le eventuali misure di sicurezza applicabili. Proprio in relazione alla normativa NIS, si può percepire l'opera di razionalizzazione posta in essere dalla riforma. Infatti, i Ministeri, le

[37] Art. 7 del d.l. n. 82/2021.

Regioni e le Province Autonome, che erano precedentemente "Autorità competenti" e che esercitavano ciascuna poteri regolamentari, di vigilanza e sanzionatori, sono adesso identificate solo come autorità di settore e, per gli ambiti di competenza, propongono all'ACN, per la sua approvazione, le variazioni all'elenco degli operatori dei servizi essenziali. I restanti poteri sono invece tutti esercitati dall'Autorità nazionale competente.

L'Agenzia agisce anche come *Computer Security Incident Response Team*, che è in essa incardinato[38]. Alla luce di ciò, essa assume un ruolo centrale nell'attività di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici. Ciò non solo ai sensi della normativa NIS, che aveva originariamente istituito il CSIRT Italia, ma anche della normativa Perimetro e di quella in materia di sicurezza delle comunicazioni elettroniche. Queste ultime hanno individuato il CSIRT Italia come l'*hub* nazionale per la segnalazione e la gestione degli incidenti, relativamente agli aspetti di resilienza *cyber*.

Con riferimento alla citata normativa in materia di comunicazioni elettroniche, l'Agenzia è autorità competente per gli aspetti di sicurezza e integrità delle stesse, definendo, ad esempio, le misure di sicurezza di settore e le soglie di significatività degli incidenti per i quali è obbligatoria la notifica[39].

L'Agenzia supporta, poi, lo sviluppo di capacità industriali, tecnologiche e scientifiche nel campo della cybersicurezza, in un'ottica di raggiungimento dell'autonomia strategica nazionale ed europea. In tale obiettivo si inseriscono le attività finalizzate all'attuazione del Piano Nazionale di Ripresa e Resilienza, che prevede apposite progettualità nell'ambito della cybersicurezza, nonché le attività svolte quale Centro nazionale di coordinamento, ai sensi del Regolamento (UE) 887/2021.

[38] Art. 7 del d.l. n. 82/2021.

[39] Artt. 40 e 41 del d. lgs. n. 259/2003, come modificato dal d. lgs. 8 novembre 2021, n. 207.

Infine, l'Agenzia esercita tutta una serie di ulteriori funzioni ad ampio spettro, tra le quali rientrano, ad esempio, l'attività di cooperazione internazionale in ambito *cyber*, il mantenimento di un quadro giuridico coerente e aggiornato in materia, la formazione, lo sviluppo della *cyberawareness* e la qualificazione dei servizi *cloud*. Queste ultime competenze giocano ciascuna un ruolo fondamentale nel raggiungere livelli più elevati di resilienza nello spazio cibernetico.

### 3.3 Il coordinamento dell'ecosistema nazionale *cyber*

Una trattazione specifica merita la funzione connessa al coordinamento interministeriale. Come illustrato in apertura dell'articolo, questo è imprescindibile per il settore della cybersicurezza, considerato che l'utilizzo di infrastrutture ICT è ormai intrinseco a tutti i settori della società e un eventuale incidente cibernetico può generare impatti sistemici. Sebbene questo coordinamento assuma preminente rilievo con riferimento al settore pubblico, esso risulta essenziale anche per gli altri ambiti dell'ecosistema nazionale, in particolare il settore privato, nonché il mondo dell'università e della ricerca, che contribuiscono ciascuno al raggiungimento di un Paese "*cyber*-sicuro" e "*cyber*-resiliente".

A tal riguardo, il Legislatore ha tenuto ben a mente queste necessità e ha previsto appositi meccanismi di coordinamento.

Primaria importanza assume l'allineamento tra le amministrazioni pubbliche, soprattutto a livello tecnico-operativo nel quale si pongono in essere le azioni concrete per prevenire e/o rimediare a eventuali danni derivanti dalla minaccia *cyber*.

A tal fine, è stato istituito presso l'ACN, in via permanente, il Nucleo per la cybersicurezza (NCS) che costituisce la principale sede di coordinamento interistituzionale a livello tecnico-operativo.

Il Nucleo è presieduto dal Direttore generale dell'ACN, che può delegare il Vice Direttore generale dell'Agenzia, ed è composto da: il Consigliere militare del Presidente del Consiglio

dei ministri; il Comparto intelligence; il Ministero degli affari esteri e della cooperazione internazionale; il Ministero dell'interno; il Ministero della giustizia; il Ministero della difesa; il Ministero dell'economia e delle finanze; il Ministero delle imprese e del made in Italy; il Ministero dell'ambiente e della sicurezza energetica; il Ministero delle infrastrutture e dei trasporti; il Ministero dell'università e della ricerca; il Dipartimento per la trasformazione digitale[40].

Il Nucleo è, al contempo, un consesso a "composizione variabile", in quanto la partecipazione allo stesso può essere ampliata o ristretta a seconda della specifica tematica oggetto di discussione. Infatti, il decreto-legge n. 82/2021 prevede, agli articoli 8 e 10, che in base agli argomenti delle riunioni, possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza. In caso di crisi di natura cibernetica, il Nucleo è integrato, in ragione della necessità, con un rappresentante, rispettivamente, del Ministero della salute e del Ministero dell'interno-Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile. Il Nucleo, inoltre, può essere convocato anche in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati.

La partecipazione modulabile si rivela particolarmente opportuna, ad esempio, nei casi in cui si verifichi un incidente cibernetico significativo ai danni di un soggetto privato che fornisce servizi essenziali. In tal caso, può essere utile invitare anche la vittima per analizzare congiuntamente potenziali effetti sistemici sui servizi impattati. L'estensione della partecipazione può essere utile anche quando sia all'ordine del giorno un'iniziativa concernente, ad esempio, un progetto di sviluppo di nuove tecnologie, per cui può essere utile invitare anche esponenti del mondo della ricerca per analizzare possibili prospettive di azione.

[40] Art. 8 del d.l. n. 82/2021.

Le considerazioni appena esposte risultano più chiare analizzando le competenze del Nucleo[41]. Infatti, sebbene il suo mandato sia l'operare a supporto del Presidente del Consiglio dei ministri per gli aspetti relativi alla prevenzione e alla preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento, il Nucleo svolge un ruolo ben più ampio. Ciò alla luce, ad esempio, del compito ad esso attribuito di poter formulare proposte di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia. Proprio l'ampiezza delle sue funzioni rende il Nucleo una sede privilegiata nella quale effettuare un allineamento tra le Amministrazioni componenti, in quanto gli altri meccanismi di cooperazione operano solo relativamente all'ambito di applicazione della normativa di settore che li istituisce, come accade, a titolo di esempio, per il Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica che tratta le sole questioni attinenti all'attuazione del PSNC.

Un altro meccanismo di coordinamento, ma con le altre componenti dell'ecosistema nazionale, è il Comitato tecnico-scientifico (CTS). Il CTS è istituito presso l'Agenzia, con funzioni di consulenza e proposta, per supportare la collaborazione con il mondo dell'università e della ricerca e con il sistema produttivo nazionale, nonché supportare le iniziative pubblico-private nell'ambito della cybersicurezza, con particolare attenzione allo sviluppo di competenze, all'innovazione, alla partecipazione a programmi e progetti di cybersicurezza nazionali e internazionali, alla promozione della *cyberawareness*, alla formazione e alla qualificazione delle risorse umane[42].

Il CTS è presieduto dal Direttore generale dell'Agenzia (ovvero dal Vice Direttore generale o da un dirigente dell'Agenzia ove delegati) e, tenuto conto del principio di pari opportunità tra uomini e donne, è composto da: a) personale dell'Agenzia in numero non superiore a quattro; b) quattro dirigenti, in rappresentanza dell'industria operativa negli ambiti di attività

[41] Art. 9 del d.l. n. 82/2021.

[42] Art. 11 del dPCM n. 223/2021.

dell'Agenzia, comprese le piccole e medie imprese; c) quattro professori universitari ordinari o equivalenti, in rappresentanza del sistema dell'università e della ricerca; d) un esponente di associazioni del settore della sicurezza delle aziende strategiche del Paese.

Grazie alla sua composizione, questo consesso rappresenta una piattaforma nella quale garantire il dialogo con le altre componenti non governative dell'ecosistema nazionale cyber, anche al fine di individuare possibili proposte e iniziative utili a sviluppare la cybersicurezza del Paese.

## 4 – Conclusioni

Il decreto-legge n. 82/2021 ha certamente rappresentato una tappa importante nella definizione di un'architettura nazionale matura e in grado di affrontare le sfide emergenti nello spazio cibernetico. Al contempo, sebbene sia riuscito a porre rimedio a diversi problemi che erano emersi nella normativa *cyber*, il lavoro non è ancora terminato. Il settore è, infatti, in costante divenire. La vera sfida per gli anni futuri sarà quella di garantire il costante e tempestivo adeguamento del quadro normativo e di *policy* nazionale ai nuovi scenari di rischio e all'evoluzione delle nuove tecnologie.

## 5 - Bibliografia

**[1]** Boschetti B., "La transizione della pubblica amministrazione", in Lalli A. (a cura di) *L'amministrazione pubblica nell'era digitale*, pp. 1- 44, 2022.

**[2]** Bonfanti M.E., "Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice", *INSS Cyber, Intelligence, and Security*, Vol. 2, No. 1, 2018, pp. 105-121.

**[3]** Montagnani E., "Le pubbliche amministrazioni nell'era delle tecnologie cloud ed edge computing tra opportunità e rischi: il Piano nazionale di ripresa e resilienza e le comunità digitali", in Abba L., Lazzaroni A. e Pietrangelo M. (a cura di), *La internet governance e le sfide della trasformazione digitale*, pp. 251-266, 2022.

**[4]** OA-Osservatorio ACCREDIA, "Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata", 2022, 1.

**[5]** Parona L., "L'istituzione dell'Agenzia per la cybersicurezza nazionale", in *Giornale Dir. Amm.*, p. 709, 2021, 6.

**[6]** Peluso F., "La disciplina italiana in tema di cybersecurity", in Contaldo A., Mula D. (a cura di) *Cybersecurity Law, Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche,* pp. 120-147, 2020.

**[7]** Relazione illustrativa al d.d.l. "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'Agenzia per la cybersicurezza nazionale".

**[8]** Renzi A., "La sicurezza cibernetica: lo stato dell'arte", in *Giornale Dir. Amm.*, p. 538, 2021, 4.

**[9]** Strategia nazionale di cybersicurezza 2022-2026.

**[10]** Decreto legislativo 1 agosto 2003, n. 259, recante "*Codice delle comunicazioni elettroniche*".

**[11]** Decreto legislativo 7 marzo 2005, n. 82, recante "*Codice dell'amministrazione digitale*".

**[12]** Decreto-legge 18 ottobre 2012, n. 179, recante "*Ulteriori misure urgenti per la crescita del Paese*".

**[13]** DPCM 24 gennaio 2013 "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*".

**[14]** DPCM 17 febbraio 2017 "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*".

**[15]** Decreto legislativo 18 maggio 2018, n. 65, "*Attuazione della 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*".

**[16]** Decreto 12 dicembre 2018 del Ministero dello sviluppo economico recante "*Misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi*".

**[17]** Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) 526/2013.

**[18]** DPCM 8 agosto 2019 recante "*Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT Italia*".

**[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*".

**[20]** DPCM 30 luglio 2020, n. 131, recante "*Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*".

**[21]** Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

**[22]** 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, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).