Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche

a cura di

Raffaella Brighi e Giovanna Adinolfi

Giappichelli

Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche


IUSTITIAM COLIMUS

Governare la sicurezza degli (eco)sistemi cyberfisici

Regolamentazione, diritti e politiche

a cura di
Raffaella Brighi e Giovanna Adinolfi

Giappichelli

VIA PO, 21 - TEL. 011-81.53.111

http://www.giappichelli.it

ISBN/EAN 979-12-211-1735-6
ISBN/EAN 979-12-211-6531-9 (ebook)

Il volume è esito del progetto di ricerca "Ecocyber - Risk management for future cyber-physical ecosystems" nell'ambito dello Spoke 8 del Paternariato esteso SERICS- SEcurity and RIghts in the CyberSpace.
Finanziato dall'Unione Europea – NextGenerationEU attraverso il Ministero dell'Università e della Ricerca italiano nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3 – Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca – D. D. 341 del 15/03/2022, PE7 SERICS – SEcurity and RIghts in the CyberSpace , Codice proposta: PE00000014, CUP: J33C22002810001,finanziato con Decreto n. 1556 del 11/10/2022.
I punti di vista e le opinioni espresse sono esclusivamente quelle degli autori e non riflettono necessariamente quelle dell'Unione Europea, né può l'Unione Europea essere ritenuta responsabile per esse.

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

G. Giappichelli Editore

Questo libro è stato stampato su carta certificata, riciclabile al 100%

Stampa: LegoDigit s.r.l. - Lavis (TN)

Indice

pag.

Capitolo 3

Il quadro della governance della cybersicurezza a livello nazionale

Tommaso F. Giupponi

pag.

Capitolo 4

La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello *jus ad bellum*

Giulia Gabrielli

Capitolo 5

Il dominio cyber negli attuali scenari di guerra mediterranei: il caso del conflitto in Medio Oriente

Riccardo Allegri, Giorgio Scichilone

Capitolo 6

Politiche di cybersicurezza e implicazioni strategiche: una lettura politologica

Luigi Martino, Giampiero Giacomello, Oltion Preka

pag.

Parte II

Cybersicurezza e protezione degli eco-sistemi cyberfisici: una visione strumentale

Capitolo 7

Gli approcci regolatori del regolamento UE in materia di (cyber)sicurezza dei prodotti: il *Cyber Resilience Act*

Pier Giorgio Chiara

Capitolo 8

Il *Cyber Resilience Act* nella prospettiva degli accordi commerciali dell'Unione europea

Giovanna Adinolfi, Rachele Magnaghi

pag.

Capitolo 9

Profili informatico-giuridici della cybersicurezza nel procurement sanitario

Marco Mancarella

Capitolo 10

Cybersicurezza e *cyber deception*: sfide e prospettive processualpenalistiche

Mariagisa Landolfi

pag.

Parte III

Cybersicurezza e tutela dei diritti fondamentali: una prospettiva critica

Capitolo 11

Polizia, *big data* e società digitale: sicurezza dei dati, sicurezza dai dati

Giulia Fabini

Capitolo 12

Il *Cyber Resilience Act* come strumento per la protezione dei valori dell'UE? Tra esigenze di sicurezza dei prodotti e tutela dei diritti fondamentali dei singoli

Virginia Remondino

pag.

Capitolo 13

Cybersecurity, indagini amministrative, cooperazione pubblico privata e processo penale. I rischi connessi ad un'era di diffusa prevenzione collaborativa

Antonio Pugliese, Giulia Lasagni

Parte IV

Consapevolezza, educazione e politiche

Capitolo 14

Cybersicurezza e fattore umano: un approccio educativo inclusivo

Antonella Carbonaro, Enrico Gnagnarella

pag.

Capitolo 15

Per un uso consapevole e sicuro delle tecnologie: strategie educative e strumenti di intervento

Valeria Barone, Thomas Casadei

pag.

Capitolo 3

Il quadro della governance della cybersicurezza a livello nazionale

Tommaso F. Giupponi [*]

Abstract: Il contributo ricostruisce, in chiave problematica, la governance della cybersicurezza a livello nazionale, frutto di una recente implementazione legislativa (anche su impulso europeo) culminata con l'istituzione dell'Agenzia per la cybersicurezza nazionale. Tale Agenzia, con funzioni di supporto tecnico e operativo rispetto alle competenze in materia della Presidenza del Consiglio dei ministri, rappresenta uno snodo centrale nel governo multilivello della cybersicurezza. Anche se collocata formalmente all'esterno del perimetro del Sistema di informazione per la sicurezza della Repubblica, molti sono gli snodi e i punti di contatto tra i due comparti, circostanza che pone la necessità di un più efficace coordinamento in materia di cybersicurezza sia all'interno del Governo, sia in relazione agli strumenti di controllo parlamentare esperibili.

Keywords: Cybersicurezza – Sicurezza nazionale – Presidenza del Consiglio dei Ministri – Agenzia per la cybersicurezza nazionale – Controllo parlamentare

1. La cybersicurezza tra ordine pubblico, difesa e sicurezza nazionale

L'evoluzione tecnologica, come noto, ha condizionato in maniera assai significativa le più recenti trasformazioni delle società contemporanee. Tale processo,

[*] Professore Ordinario di Diritto Costituzionale presso il Dipartimento di Scienze Giuridiche dell'Università di Bologna, tommaso.giupponi@unibo.it.

tra le altre cose, ha imposto anche una rilettura di alcune delle categorie giuridiche più consolidate, al fine di adeguarle alla continua (e sempre più rapida) innovazione, giungendo a ridefinire il ruolo stesso degli Stati come comunità politiche organizzate, non solo, sul piano interno, quali veri e propri Stati digitali [1], ma anche sul piano internazionale. Gli strumenti messi a disposizione dall'*Information and Communication Technology* (ICT), alla luce delle loro immense potenzialità, hanno da subito fatto emergere non solo nuovi orizzonti di sviluppo della persona umana e dei suoi diritti fondamentali, ma hanno parallelamente posto un enorme problema di tutela e regolazione rispetto ai rischi connessi ad un loro utilizzo massiccio ed incontrollato.

Alle tradizionali minacce sperimentate nell'arena "materiale" di espressione della sovranità degli Stati, cui tradizionalmente gli ordinamenti hanno risposto attraverso la predisposizione di specifici strumenti ed apparati amministrativi (si pensi, solo per fare un esempio, alla difesa e all'ordine pubblico), si aggiungono ora nuove vulnerabilità dovute all'utilizzo sempre più diffuso dell'ICT nell'ambito delle nuove arene "virtuali", fortemente interconnesse tra loro, le quali rappresentano ormai il terreno privilegiato di azione di singoli individui, operatori economici e pubbliche autorità [2], in un contesto dove i tradizionali confini tra sicurezza interna ed esterna sembrano divenire, a tratti, sempre più sfumati [3].

Anche i pubblici poteri, infatti, utilizzano ormai diffusamente tali strumenti nell'esercizio delle loro funzioni istituzionali, mentre la maggior parte dei servizi essenziali è oggi garantita, organizzata ed erogata grazie alla rete ed alle tecnologie informatiche. Rispetto alle tradizionali infrastrutture "materiali", tuttavia, le infrastrutture "virtuali" evidenziano differenti problemi di tutela rispetto alle potenziali minacce, che richiedono la costruzione di un adeguato impianto normativo, ad alto contenuto tecnico. Proprio per questo, il problema della sicurezza delle reti e degli strumenti di comunicazione è divenuto oggi un problema centrale [4].

---

[1] Sul punto, da ultimo, cfr. L. TORCHIA, *Lo Stato digitale. Una introduzione*, Il Mulino, Bologna, 2025.

[2] R. BALDONI, *Sovranità digitale. Cos'è e quali sono le principali minacce al cyberspazio nazionale*, Il Mulino, Bologna, 2025.

[3] Sul punto, per tutti, G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, 2019, n. 4, p. 65 ss.

[4] Secondo il *Rapporto CLUSIT* del 2025, il numero di incidenti informatici rilevati in Italia nel 2024 è aumentato del 15,2% rispetto al 2023, con una tendenza che è comunque in significativo aumento da anni anche a livello globale (www.clusit.it). Sul punto, vedi anche l'ultima *Relazione sull'attività svolta dall'Agenzia per la cybersicurezza nazionale* (presentata al Parlamento il 2 maggio 2025), in base alla quale sono stati rilevati, nel corso del 2024, ben 1.979 eventi *cyber*, con un aumento del 40% rispetto al 2023.

Non è un caso, allora, che sia stato sottolineato come la cybersicurezza [5] assuma oggi tutte le caratteristiche di una vera e propria funzione pubblica, del tutto peculiare, e che rappresenti un possibile nuovo "volto" del potere negli Stati costituzionali liberaldemocratici [6].

È del tutto evidente, infatti, che tale evoluzione ha ridisegnato anche il piano delle relazioni internazionali; nell'attuale scenario politico globale, infatti, gli Stati si fronteggiano non solo nell'ambito dei più tradizionali "domini" consolidati (terrestre, marino, aereo e spaziale), ma anche nel nuovo dominio *cyber*, vero e proprio spazio virtuale interconnesso, dove sempre di più essi agiscono anche nella gestione e risoluzione dei conflitti e delle controversie internazionali, di fronte a minacce di natura sempre più ibrida (si pensi, solo per fare qualche esempio, alla *cyber warfare* e alla *cyber intelligence*) [7].

In questo contesto, non stupisce allora che la *cyber security* (o cybersicurezza) evidenzi più di un collegamento con la tutela della sicurezza nazionale e con gli apparati tradizionalmente posti a sua tutela dagli ordinamenti nazionali. Tuttavia, proprio per la sua trasversalità, il dominio *cyber* richiede parallelamente il coinvolgimento di altri apparati dello Stato, quali l'amministrazione di pubblica sicurezza e quella della difesa, oltre che un significativo apporto degli operatori economici privati.

D'altronde, come noto, lo stesso concetto di sicurezza nazionale ha subito negli ultimi decenni un'evoluzione che ne ha ridefinito natura e confini, anche alla luce della necessità di un suo adeguamento rispetto alle nuove minacce emergenti sullo scenario globale, come il terrorismo internazionale e la stessa criminalità informatica [8]. In questo senso, allora, non è un caso che l'attuale

---

[5] Per un inquadramento del tema, cfr. G. D'ANGELO-G. GIACOMELLO, *Cybersicurezza. Che cos'è e come funzione*, Il Mulino, Bologna, 2023; nonché, con specifico riferimento agli aspetti informatico-giuridici, R. BRIGHI, *Introduzione al concetto di cybersicurezza: una prospettiva informatico-giuridica*, in questo volume.

[6] In questo senso, da ultimo, R. URSI, *La sicurezza cibernetica come funzione pubblica*, in Ursi, R. (a cura di), *op. cit.*, p. 7 ss.; E. LONGO, *Il diritto costituzionale e le cybersicurezza. Analisi di un volto nuovo del potere*, in *Rassegna parlamentare*, 2024, n. 2, p. 313 ss. Sul punto, con uno sguardo alle dinamiche europee, vedi anche R. BRIGHI-P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi.it*, 2021, n. 21, p. 18 ss.

[7] Negli ultimi anni tale tendenza si è manifestata non solo in relazione all'emergenza terroristica internazionale ma, più di recente, anche in occasione di veri e propri conflitti armati, come quello russo-ucraino, e attraverso campagne di disinformazione e di diffusione in rete di *fake news*, volte ad influenzare l'opinione pubblica. Sul punto, da ultimo, vedi la *Relazione annuale sulla politica dell'informazione per la sicurezza* del 2024 (XIX Legislatura, Doc. XXXIII, n. 3), in particolare p. 21 ss., www.sicurezzanazionale.gov.it; www.parlamento.it.

[8] Sul punto, sia consentito un rinvio a T.F. GIUPPONI, *Sicurezza e potere*, in *Enciclopedia del diritto*, *I Tematici*, *Potere e Costituzione*, V, Giuffrè, Milano, 2023, p. 1146 ss.

disciplina in materia di servizi di informazione e segreto di Stato individui, tra le finalità principali di tale particolare apparato normativo, la «integrità della Repubblica, anche in relazione ad accordi internazionali», la «difesa delle istituzioni poste dalla Costituzione a suo fondamento», la «indipendenza […] rispetto agli altri Stati», la «preparazione» e la «difesa militare» [9]. Quanto alle attività dei servizi di *intelligence*, invece, alle due Agenzie viene affidato il compito di acquisire ed analizzare le informazioni volte a proteggere la Repubblica da minacce esterne ed interne (anche rispetto ad attività eversive o terroristiche), al fine di garantire «la protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia» [10]. Infine, si prevede che ai servizi di informazione sia affidata in via esclusiva anche l'attività di controspionaggio, finalizzata a contrastare le attività informative «volte a danneggiare gli interessi nazionali» [11].

Oggi, infatti, l'indipendenza e la sovranità di uno Stato possono essere messe in discussione non solo sul piano dell'aggressione armata o dell'attacco terroristico, ma anche sul piano economico, finanziario, industriale o tecnologico [12]: il riferimento obbligato va, ad esempio, alla stabilità del sistema economico generale, alla sicurezza informatica delle strutture strategiche nazionali, fino ai variegati interessi scientifici e tecnologici convolti dalla c.d. sicurezza sanitaria ed alla accessibilità delle fonti di approvvigionamento energetico, resi evidenti dalla pandemia da Covid-19 e dal più recente conflitto tra Russia e Ucraina. Sullo sfondo, emerge anche la disciplina dei "poteri speciali" del Governo nei settori strategici per la tutela degli interessi nazionali quali la difesa, la sicurezza nazionale, l'energia i trasporti e le comunicazioni (c.d. *golden power*), che ha subito un processo di progressiva implementazione ed estensione, da ultimo proprio in relazione all'evoluzione dei servizi ICT e ai connessi profili di sicurezza cibernetica [13].

---

[9] Così, in particolare, l'art. 39, comma 1, della l. n. 124/2007.

[10] In questo senso, espressamente, gli artt. 6, comma 2, e 7, comma 2, della l. n. 124/2007.

[11] Cfr. gli artt. artt. 6, comma 3, e 7, comma 3, della l. n. 124/2007.

[12] Il dato appare evidente anche dalla lettura della *Relazione sulla politica dell'informazione per la sicurezza* che il Presidente del Consiglio deve presentare al Parlamento entro la fine di febbraio di ogni anno (art. 38 della l. n. 124/2007). Negli ultimi anni, infatti, è emersa progressivamente sempre una maggiore attenzione ai profili di sicurezza economico-finanziaria, energetica ed ambientale, oltre che in materia di *cybersecurity*, anche alla luce della natura sempre più ibrida delle minacce alla sicurezza nazionale. Da ultimo, vedi la già citata *Relazione* annuale, presentata lo scorso 28 febbraio 2025.

[13] Sulla base di quanto previsto dal d.l. n. 21/2012, più volte modificato. Su tali aspetti, si vedano, tra gli altri, B. CAROTTI, *Sicurezza cibernetica e Stato-nazione*, in *Giornale di diritto amministrativo*, 2020, n. 5, p. 629 ss.; G. DELLA CANANEA-L. FIORENTINO (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Napoli, Editoriale scientifica, 2020; C. GENGARO,

Tale lettura sembra ora trovare una qualche conferma anche nel dettato normativo. Istituendo l'Autorità per la cybersicurezza nazionale (ACN), infatti, il legislatore ha colto l'occasione per definire la *cyber security* come «l'insieme delle attività […] necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, *anche* ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico»; tuttavia, viene espressamente specificato che rimangono ferme le attribuzioni del Sistema di informazione per la sicurezza della Repubblica e gli obblighi derivanti dai trattati internazionali [14].

Dunque, come vedremo, la cybersicurezza evoca un ambito di intervento piuttosto ampio, multilivello e trasversale, all'interno del quale sono innegabili i collegamenti con il sistema di informazione per la sicurezza, ma che non può essere fatto coincidere, *sic et simpliciter*, con l'area operativa dell'*intelligence*, non fosse altro perché il processo di trasformazione digitale dell'amministrazione pubblica attualmente in corso riguarda trasversalmente tutti i settori, e chiama inevitabilmente in causa anche l'attività degli operatori economici e delle imprese private coinvolte in tale processo [15].

Tuttavia, è fuori discussione che (almeno alle origini) la normativa italiana in materia di *cyber security* sia nata all'interno del Sistema di informazione per la sicurezza della Repubblica, disciplinato, come noto, dalla l. n. 124/2007. Infatti, alla luce delle modifiche introdotte dalla l. n. 133/2012, tra i compiti affidati al Presidente del Consiglio dei ministri, quale Autorità nazionale per la sicurezza della Repubblica, troviamo oggi anche quello di impartire al Dipartimento delle informazioni per la sicurezza (DIS) e alle agenzie di *intelligence* «direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali» [16].

Stato e mercato. Dalla golden share al golden power, Napoli, Editoriale scientifica, 2023. Sul punto, vedi anche quanto previsto dal Regolamento (UE) n. 2019/452 sul controllo degli investimenti esteri diretti all'interno dell'UE, sul quale cfr. G. NAPOLITANO (a cura di), *Foreign Direct Investment Screening. Il controllo sugli investimenti esteri diretti*, Bologna, Il Mulino, 2019.

[14] Vedi quanto stabilito dall'art. 1, comma 1, lett. a), del d.l. n. 82/2021.

[15] Sul punto, tra gli altri, si veda L. PREVITI, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informativo*, in *Federalismi.it*, 2022, n. 25, p. 65 ss.

[16] In questo senso l'art. 1, comma 3-*bis*, della l. n. 124/2007, introdotto dalla l. n. 133/2012. A sua volta, il DIS (sulla base di tali direttive) «coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali»; cfr. l'art. 4, comma 3, lett. d-*bis*) della l. n. 124/2007, come modificata dalla già citata l. n. 133/2012. Sulla base di tali previsioni, sono stati adottati i primi provvedimenti in materia di cybersicurezza (cfr.

Tuttavia, la complessità (non solo tecnica) della materia e la necessità di un maggiore coordinamento tra le diverse istituzioni coinvolte, oltre che il particolare rilievo delle imprese private operanti nel settore, hanno fatto emergere molto presto l'impossibilità di una collocazione esclusiva della *cyber security* all'interno del comparto *intelligence*. Questo, a ben vedere, non tanto perché l'attività informativa a tutela della sicurezza nazionale non debba, oggi più che mai, confrontarsi anche con le potenzialità (e le minacce) della rete e delle tecnologie informatiche di comunicazione, quanto perché la progressiva evoluzione tecnologica dell'amministrazione, dei servizi pubblici, delle attività economiche e delle più generali relazioni sociali rende necessario garantire trasversalmente la sicurezza *delle* reti e degli stessi utenti *nelle* reti.

Questa consapevolezza, come vedremo, ha portato l'ordinamento ad un progressivo cambio di passo che, a partire dalle indicazioni provenienti dall'UE, ha recentemente rivisto la complessiva architettura istituzionale della cybersicurezza, attraverso un percorso che, tuttavia, appare ancora in atto e non privo di ambiguità ed incertezze.

2. L'evoluzione della normativa di settore e la sua progressiva stratificazione (e complicazione)

Nella consapevolezza dell'insufficienza di ogni tentativo di regolazione a livello nazionale [17], l'attenzione dell'UE in materia è andata via via crescendo nel corso degli anni, anche al fine di garantire un mercato unico delle tecnologie digitali, assicurando l'affidabilità degli strumenti ITC e *standard* uniformi di protezione degli utenti. Infatti, a partire dall'adozione di una vera e propria strategia europea in materia di *cyber security*, sono stati approvati negli ultimi anni diversi atti normativi particolarmente significativi, volti non solo ad accompagnare la transizione digitale e l'innovazione tecnologica attraverso la garanzia di strumenti affidabili, ma anche a rafforzare la capacità dell'UE e degli Stati membri di resistere a possibili attacchi informatici [18].

---

il d.p.c.m. 24 gennaio 2013 e il successivo d.p.c.m. 17 febbraio 2017, recanti indirizzi per la protezione cibernetica e la sicurezza informatica nazionale), i quali prevedevano una complessa architettura istituzionale, incentrata sulla Presidenza del Consiglio dei ministri, sul DIS, sul Comitato interministeriale per la sicurezza della Repubblica (CISR) nonché, per i profili più squisitamente tecnico-operativi, sul Nucleo per la sicurezza cibernetica (NSC).

[17] Tra le risposte a livello internazionale, si segnala in particolare la Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest nel 2001, entrata in vigore nel 2004 e attualmente ratificata da 69 paesi (per l'Italia, cfr. la l. n. 48/2008).

[18] Sul punto, tra gli altri, si veda E. LONGO, *La disciplina della cybersicurezza nell'Unione*

Due, sostanzialmente, le direttrici seguite: 1) armonizzare gli *standard* di sicurezza previsti dagli ordinamenti nazionali in materia di prevenzione delle (e risposta alle) minacce informatiche in alcuni settori strategici considerati particolarmente rilevanti; 2) rafforzare gli strumenti di cooperazione, prevedendo parallelamente un sistema europeo di certificazione in materia di cybersicurezza, in modo da creare un mercato unico dei relativi servizi.

Sul primo punto, in particolare, è intervenuta dapprima la Direttiva (UE) n. 2016/1148 (*Network and Information Security*, c.d. NIS), attuata tramite il d.lgs. n. 65/2018, recentemente sostituita dalla Direttiva (UE) n. 2022/2555, c.d. NIS 2, attuata dal d.lgs. n. 138/2024. Sul secondo, invece, assumono particolare rilevanza il Regolamento (UE) n. 2019/881 (c.d. *Cybesecurity Act*) nonché, da ultimo, il Regolamento (UE) n. 2024/2847 (c.d. *Cyber Resilience Act*) e il Regolamento (UE) n. 2025/38 (c.d. *Cyber Solidarity Act*). Comune a tutti i più recenti interventi dell'UE in materia, in ogni caso, è il tentativo di un superamento del tradizionale approccio settoriale che aveva contraddistinto i precedenti interventi in materia, attraverso una visione trasversale e multisettoriale alla cybersicurezza [19].

Con le Direttive NIS e NIS 2, in particolare, al fine di introdurre una disciplina minima comune in materia di sicurezza delle reti e dei servizi informativi, sono stati previsti tutta una serie di obblighi in capo agli Stati e ai soggetti operanti nell'ambito dei settori individuati come essenziali e strategici [20].

Quanto agli Stati, è previsto che essi debbano adottare una strategia nazionale in materia di cybersicurezza «per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale», all'interno della quale, tra l'altro, indicare gli obiettivi e le priorità da seguire, il quadro di *governance* previsto, un sistema di valutazione dei rischi, le misure di preparazione, risposta e recupero rispetto

---

europea e in Italia, in S. CALZOLAIO-A. IANNUZZI-E. LONGO-M. OROFINO (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 203 ss.; per una ricostruzione dell'evoluzione normativa europea in materia di cybersicurezza, vedi anche F. CASOLARI-F. FERRI-S. VILLANI, *La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea*,in questo volume.

[19] Vedi, tuttavia, ora il Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act*), il quale prevede prescrizioni specifiche in materia di cybersicurezza per il settore finanziario (sul punto, da ultimo, vedi anche il d.lgs. n. 23/2025).

[20] Con particolare riferimento ai settori dell'energia, dei trasporti, bancario e dei servizi finanziari, di fornitura e distribuzione di acqua, delle infrastrutture digitali (cf. l'Allegato II del d.lgs. n. 65/2018). La Direttiva NIS 2, da ultimo, ha esteso il suo campo di applicazione anche ad altri significativi settori, quali quello sanitario, l'ingegneria aerospaziale, la gestione dei rifiuti, la produzione e distribuzione alimentare, il settore chimico, i servizi postali, le organizzazioni di ricerca, ma anche buona parte della pubblica amministrazione (cfr. gli Allegati I, II, III e IV del d.lgs. n. 138/2024).

alle minacce informatiche, oltre che specifici piani di formazione, sensibilizzazione e ricerca in materia di sicurezza delle reti e dei sistemi informativi [21]. Sempre in capo agli Stati, poi, è previsto l'obbligo di individuare una o più Autorità nazionali in materia di sicurezza informatica, di istituire uno specifico gruppo di intervento per la sicurezza in caso di incidente informatico (*Computer Security Incident Response Team*, c.d. CSIRT), oltre che di prevedere un punto di contatto unico nazionale per garantire un'efficace cooperazione tra l'UE e gli Stati membri [22].

In relazione ai soggetti operanti nell'ambito dei già citati settori strategici, vengono individuati specifici obblighi per i soggetti definiti «essenziali» e per quelli definiti «importanti», con una gradazione che tiene conto del livello di criticità dello specifico settore e della sua interconnessione con altri settori o servizi considerati strategici [23].

Tali soggetti, in particolare, devono adottare misure organizzative e tecniche adeguate e proporzionate per evitare, fronteggiare e gestire eventuali attacchi (o incidenti) informatici diretti alle proprie infrastrutture digitali, notificando al CSIRT Italia gli eventuali episodi che abbiano un impatto rilevante sulla continuità dei servizi forniti [24]. In caso di inadempimento, sono previste specifiche sanzioni amministrative pecuniarie [25].

Quanto al secondo punto, invece, il *Cybersecurity Act* è intervenuto in una duplice direzione, rafforzando il ruolo dell'*European Network and Information Security Agency* (ENISA) [26], e introducendo un quadro comune europeo per la

---

[21] In questo senso, da ultimo, vedi l'art. 9 del d.lgs. n. 138/2024.

[22] Cfr. ora gli artt. 10 e 15 del d.lgs. n. 138/2024, che individuano l'Agenzia per la cybersicurezza nazionale (ACN) quale autorità nazionale e punto di contatto unico, disciplinando al contempo organizzazione e funzionamento del CSIRT Italia.

[23] Tra i primi rientrano, ad esempio, gli operatori del settore energetico, sanitario, spaziale, bancario, dei trasporti, delle infrastrutture digitali e delle acque, oltre che le pubbliche amministrazioni centrali; tra i secondi, invece, sono ricompresi (tra gli altri) i servizi postali, la gestione dei rifiuti, il settore chimico, quello agroalimentare e le organizzazioni di ricerca, cui si aggiungono anche le pubbliche amministrazioni territoriali specificamente individuate (cfr. l'art. 6 del d.lgs. n. 138/2024).

[24] Sul punto, in particolare, si vedano gli artt. 24 e 25 del d.lgs. n. 138/2024. In particolare, è previsto che senza ingiustificato ritardo, e comunque entro 24 ore, debba essere inviata al CSIRT Italia una pre-notifica dell'incidente informatico, seguita da una notifica più dettagliata entro 72 ore, contenente una prima valutazione dell'incidente stesso.

[25] Cfr. l'art. 38 del d.lgs. n. 138/2024.

[26] Istituita (pur provvisoriamente e con limitate funzioni consultive) dal Regolamento (CE) n. 2004/460 e successivamente riformata dal Regolamento (UE) n. 2013/526, oggi l'ENISA svolge un ruolo fondamentale, dovendo supportare gli Stati nell'elaborazione ed attuazione delle politiche di cybersicurezza.

certificazione della sicurezza di prodotti e servizi ICT, mentre il *Cyber Resilience Act* ha introdotto regole volte ad aumentare la sicurezza e resilienza informatica dei prodotti con elementi digitali. Da ultimo, il *Cyber Solidarity Act* ha implementato gli strumenti di cooperazione operativa in relazione agli incidenti informatici aventi un impatto significativo e su larga scala.

In questo senso, appare particolarmente significativa la previsione di una vera e propria rete composta dai diversi gruppi di intervento nazionali per la sicurezza in caso di incidente (c.d. CSIRTs *Network*), cui partecipa anche il gruppo di intervento della stessa UE (c.d. CERT-UE), e il cui Segretariato è incardinato presso l'ENISA [27]. Parallelamente, sempre presso l'ENISA è stato istituito il Segretariato dell'*EU Cyber Crisis Liaison Organization Network* (c.d. EU-CyCLONE), avente lo scopo di garantire una più stretta collaborazione, un costante scambio informativo e un'azione coordinata tra le autorità competenti a gestire le crisi informatiche a livello nazionale, in caso di incidenti su larga scala [28].

A sua volta, il legislatore nazionale è successivamente intervenuto più volte, dapprima attraverso l'istituzione del Perimetro di sicurezza nazionale cibernetica (PSNC), ad opera del d.l. n. 105/2019 [29], nonché, da ultimo, con l'approvazione della l. n. 90/2024, contenente una serie di misure eterogenee miranti a rafforzare la cybersicurezza nazionale [30]. Tali ripetuti interventi, unitamente alla necessità di un costante adeguamento ai provvedimenti europei già citati, hanno finito per costruire un quadro normativo particolarmente complesso ed articolato, a tratti di difficile ricostruzione e non privo di contraddizioni.

---

[27] Come già previsto dall'art. 12, comma 2, della Direttiva NIS, confermato dall'art. 7, comma 3, del *Cybersecurity Act*, e attualmente ribadito anche dall'art. 15 della Direttiva NIS 2. Sul punto, vedi ora anche quanto previsto dall'art. 3 del *Cyber Solidarity Act*, nell'istituire il sistema europeo di allerta per la cybersicurezza.

[28] In base a quanto stabilito dall'art. 16 della Direttiva NIS 2. Secondo quanto ora previsto dall'art. 13 del d.lgs. n. 138/2024, l'ACN e il Ministero della difesa "sono individuati quali Autorità nazionali di gestione delle crisi informatiche", rispettivamente, per la parte relativa alla resilienza nazionale e per la parte relativa alla difesa dello Stato, riconoscendo però una funzione di coordinamento in capo alla stessa ACN.

[29] Su tale intervento normativo, tra gli altri, si vedano S. POLETTI, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro nazionale di sicurezza cibernetica*, in *MediaLaws*, 2023, n. 2, p. 398 ss.; L. CALANDRIELLO, *Il perimetro di sicurezza nazionale cibernetica*, in R. URSI (a cura di), *op. cit.*, p. 139 ss.

[30] Rafforzando il livello di sicurezza informatica, con particolare riferimento alle pubbliche amministrazioni, intervenendo sulla governance della cybersicurezza, potenziando il coordinamento tra i vari soggetti istituzionali coinvolti e affinando, altresì gli strumenti di tutela penale in materia. Su tale provvedimento legislativo, da ultimo, si vedano le osservazioni critiche di L. PREVITI, *La nuova legge sulla cybersicurezza, un passo avanti e due indietro*, in *Giornale di diritto amministrativo*, 2025, n. 1, p. 60 ss.

La finalità dell'istituzione del PSNC, esplicitata fin dalle prime righe del d.l. n. 105/2019, è stata quella di «assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi 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» [31].

Il provvedimento in questione ha cercato di dare una risposta unitaria e coordinata alle minacce *cyber* in grado di compromettere la sicurezza nazionale in relazione a settori considerati strategici. Tuttavia, l'architettura istituzionale delineata, oltre che la concreta attuazione delle misure previste dal PSNC, sono apparse subito molto complesse, essendo coinvolte diverse amministrazioni dello Stato, oltre che enti e operatori pubblici e privati, ed essendo richiesti diversi provvedimenti di attuazione del quadro legislativo delineato [32]. In ogni caso, centrale (ancora una volta) è il ruolo della Presidenza del Consiglio dei ministri e del Sistema di informazione per la sicurezza della Repubblica, pur essendo previsto (almeno originariamente) un coinvolgimento importante anche del Ministero dello sviluppo economico, con particolare riferimento alla valutazione e certificazione dei sistemi e servizi ICT [33].

Particolarmente delicata, come può facilmente intuirsi, è l'individuazione delle categorie di soggetti ricompresi nel PSNC, la quale viene demandata (quanto ai criteri generali) ad un apposito d.p.c.m., mentre per l'indicazione puntuale di coloro che rientrano nel perimetro è prevista l'adozione di uno specifico provvedimento amministrativo segretato, sempre da parte del Presidente del Consiglio dei ministri [34]. In base al d.p.c.m. n. 131/2020, «un soggetto esercita una funzione essenziale dello Stato […] laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le

[31] Così, espressamente, l'art. 1 del d.l. n. 105/2019.

[32] Cfr., in questo senso, il d.p.c.m. n. 131/2020, il d.p.r. n. 54/2021, il d.p.c.m. n. 81/2021, il d.p.c.m. 15 luglio 2021 nonché, da ultimo, il d.p.c.m. n. 92/2022.

[33] Di competenza del Centro di valutazione e certificazione nazionale (CVCN), previsto dall'art. 1, comma 6, del d.l. n. 105/2019.

[34] Si veda, in questo senso, l'art. 1, comma 2-*bis*, del d.l. n. 105/2019, in base al quale l'elencazione dei soggetti inclusi nel PSNC «è contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri […] per il quale è escluso il diritto di accesso» e che «non è soggetto a pubblicazione, fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco» (vedi, sul punto, anche l'art. 5 del d.p.c.m. n. 131/2020).

relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti»; mentre «presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato […] laddove ponga in essere: attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale» [35].

A tali soggetti la normativa richiede non solo l'adozione di adeguate misure tecniche ed organizzative, finalizzate ad un monitoraggio costante del rischio cui le loro infrastrutture informatiche sono potenzialmente esposte [36], ma richiede anche una tempestiva notifica al CSIRT degli eventuali incidenti aventi un impatto sui beni ICT relativi alle proprie reti o ai propri sistemi informativi identificati come parte del Perimetro [37]. Anche in questo caso, a fronte del mancato rispetto degli obblighi in questione, sono previste significative sanzioni amministrative, anche pecuniarie, a carico dei soggetti inadempienti [38].

Dunque, una disciplina che sembra in parte seguire il modello della normativa NIS, con la previsione di specifici obblighi, dei connessi controlli e di eventuali sanzioni in caso di inadempienza. Tuttavia, come abbiamo visto, la

---

[35] In questo senso, espressamente, l'art. 2, comma 1, del d.p.c.m. n. 131/2020. In base al successivo art. 3, «ai fini dell'inclusione nel perimetro, sono oggetto di individuazione […], fatta salva l'estensione ad altri settori […], i soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni CISR, nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività […]: a) interno; b) difesa; c) spazio e aerospazio; d) energia; e) telecomunicazioni; f) economia e finanza; g) trasporti; h) servizi digitali; i) tecnologie critiche […]; l) enti previdenziali/lavoro».

[36] Come, ad esempio, predisporre e aggiornare (almeno una volta all'anno) l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, formato sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto dei diversi settori di attività, procedendo ad una valutazione del rischio connesso ai singoli beni così individuati (cfr. l'art. 1, comma 2, lett. b), del d.l. n. 105/2019, nonché l'art. 7 del d.p.c.m. n. 131/2020).

[37] Sulla base di quanto previsto dall'art. 1, comma 3, lett. a) del d.l. n. 105/2019, così come attuato dal successivo d.p.c.m. n. 81/2021, il quale ha distinto tra notifiche obbligatorie (art. 3) e notifiche volontarie (art. 4). Da ultimo, il d.l. n. 115/2022, ha esteso gli obblighi di notifica anche in caso di incidenti riguardanti *asset* che, sebbene non riguardanti direttamente il PSNC, siano comunque di pertinenza dei soggetti in esso ricompresi (vedi l'attuale art. 1, comma 3-*bis*, del d.l. n. 105/2019).

[38] Cfr. l'art. 1, commi 9 ss., del d.l. n. 105/2019.

regolamentazione del PSNC non si sostituisce, ma si affianca a quella delle Direttive NIS e NIS 2, cosa che ha creato diversi problemi di coordinamento, dal momento che le Autorità competenti, gli strumenti di intervento ed i soggetti coinvolti non sono sempre i medesimi [39]. Di qui, a ben vedere, l'urgenza di un intervento normativo finalizzato a dare maggiore coerenza all'architettura nazionale in materia di cybersicurezza, anche per garantire una maggiore efficacia di fronte all'aumento esponenziale della minaccia informatica.

Al momento, però, non sembra che questa sia la strada intrapresa dal legislatore, se solo si pensa a quanto previsto dalla già citata l. n. 90/2024. Con tale provvedimento legislativo, infatti, si sono sostanzialmente anticipati nei confronti delle pubbliche amministrazioni espressamente indicate [40], molti dei contenuti della Direttiva NIS 2 (che sarebbe stata attuata pochi mesi dopo dal già citato d.lgs. n. 138/2024), circostanza che sottolinea ancora una volta la necessità di una maggiore organicità di intervento, vista anche la delicatezza della materia, al fine di evitare potenziali duplicazioni e sovrapposizioni tra procedure che si sono via via stratificate nel corso degli ultimi anni. In ogni caso, appare particolarmente significativa la previsione dell'obbligo, per le pubbliche amministrazioni in questione, di individuare un'apposita struttura organizzativa in materia di cybersicurezza, al cui vertice viene posto il c.d. referente per la sicurezza, soggetto responsabile dell'ufficio e dotato di specifiche competenze tecniche e professionali [41].

---

[39] Anche per questo, come noto, non sono mancati interventi di coordinamento tra le due discipline; si veda, da ultimo, quanto ora ribadito dall'art. 43, comma 2, lett. b), del d.lgs. n. 138/2024, il quale prevede che le notifiche di incidente dei soggetti ricompresi nel PSNC, e i quali ricadano contemporaneamente nell'ambito di applicazione della normativa NIS, assolvono anche agli obblighi di notifica di incidente previsti da quest'ultima. Come noto, infatti, la normativa relativa al PSNC stabilisce termini temporali per la notifica molto più ristretti: 6 ore o, addirittura, 1 ora a seconda della tipologia di incidente (cfr. l'art. 3, comma 4, del d.p.c.m. n. 81/2021).

[40] Per l'individuazione delle quali si veda l'art. 1 della l. n. 90/2024. In ogni caso, tali amministrazioni ricadono oggi tutte anche nel campo di applicazione della già citata Direttiva NIS 2 (si vedano, in particolare, gli Allegati III e IV del d.lgs. n. 138/2024 i quali indicano, tra l'altro, gli organi costituzionali e di rilievo costituzionale, la Presidenza del Consiglio ed i Ministeri, le Regioni, le Province autonome, le Città metropolitane e i Comuni con più di 100.000 abitanti).

[41] Cfr. l'art. 8 della l. n. 90/2024. Tuttavia, il fatto che la legge in questione preveda espressamente una clausola di invarianza finanziaria (art. 24, comma 1), unitamente all'esplicita previsione che «la struttura e il referente […] possono essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione digitale» già previsti dal Codice dell'amministrazione digitale, di cui al d.lgs. n. 82/2005, non fa ben sperare quanto all'implementazione della previsione in questione.

3. L'Agenzia per la cybersicurezza nazionale e il ruolo della Presidenza del Consiglio dei ministri. I rapporti con il Sistema di informazione per la sicurezza della Repubblica

Al cuore della *governance* nazionale della *cybersecurity*, è posta l'Agenzia per la cybersicurezza nazionale (ACN), istituita dal d.l. n. 82/2021 [42]. La scelta di istituire un organismo specifico per coordinare i diversi attori operanti in questo delicato settore, a ben vedere, sembra rispondere a due necessità di fondo: da un lato, superare il disorganico quadro normativo precedentemente in vigore, con una moltiplicazione di soggetti ed una non sempre chiara ripartizione di competenze, in molti casi ad alto contenuto tecnico; dall'altro, svincolare la gestione della sicurezza cibernetica dall'apparato di *intelligence*, cui era stato sostanzialmente affidato (come abbiamo visto) fin dalla l. n. 133/2012, con tutti i problemi legati alla gestione delle attività di vigilanza, certificazione e controllo che coinvolgono anche soggetti privati, oltre che ai delicati rapporti con le eventuali indagini dell'Autorità giudiziaria [43].

---

[42] Sul punto, cfr. F. SERINI, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, 2022, n. 12, p. 241 ss.; I. FORGIONE, *Il ruolo strategico dell'Agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in R. Ursi (a cura di), *op. cit.*, p. 95 ss.; nonché, volendo, T.F. GIUPPONI, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2024, n. 2, p. 287 ss.

[43] In tal senso, si veda quanto stabilito dall'art. 17, comma 4, del d.l. n. 82/2021, in base al quale «il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale», essendo pertanto tenuto alla trasmissione delle notifiche di incidente ricevute al Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) della Polizia di Stato. Inoltre, è previsto anche che «l'Agenzia trasmette al Procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti» ai fini dell'esercizio delle sue funzioni, *ex* art. 371-*bis* c.p.p. (così l'art. 17, comma 4-*bis*, del medesimo d.l., così come modificato dal d.l. n. 105/2023). Da ultimo, la già citata l. n. 90/2014 ha ulteriormente specificato le forme di doverosa collaborazione tra ACN, forze di polizia e autorità giudiziaria prevedendo, tra l'altro, che, in relazione ad attacchi ai danni di sistemi informatici di cui all'art. 371-*bis*, comma 4-*bis*, c.p.p., o che interessino i soggetti inclusi nel PSNC o quelli ricompresi ambito NIS, l'Agenzia informi «senza ritardo» il Procuratore nazionale antimafia e antiterrorismo. Parallelamente, e quasi specularmente, quando il pubblico ministero acquisisce la notizia di delitti di cui al già citato art. 371-*bis*, comma 4-*bis*, c.p.p., ne deve dare «tempestiva informazione» all'ACN, contemperando lo svolgimento delle attività di indagine con le azioni avviate dall'Agenzia «a fini di resilienza» nell'ambito delle sue competenze; tuttavia, se necessario, può disporre il differimento di uno o più delle predette attività dell'ACN per evitare un grave pregiudizio per il corso delle indagini (cfr., l'art. 22 della l. n. 90/2014, nel modificare l'art. 17 del d.l. n. 82/2021). Sul punto, si vedano F.N. RICOTTA, *Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'autorità giudiziaria*, in *Diritto penale contemporaneo*, 2023, n. 1, p 97 ss.; nonché A. PUGLIESE-G. LASAGNI,

Tuttavia, alla luce della rilevanza strategica della cybersicurezza, il provvedimento legislativo in questione ha confermato, ancora una volta, il ruolo centrale della Presidenza del Consiglio dei ministri cui spetta, in via esclusiva, «l'alta direzione e la responsabilità generale delle politiche di cybersicurezza», l'adozione della relativa «strategia nazionale», vero e proprio documento programmatico fondamentale in materia [44], oltre che la nomina e la revoca del Direttore generale e del Vice Direttore generale della stessa ACN, previa deliberazione del Consiglio dei ministri [45]. Alla luce di questo suo ruolo, il Presidente del Consiglio può impartire specifiche direttive in materia di cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione ed il funzionamento dell'ACN [46]. Al di fuori delle funzioni che gli spettano in via esclusiva, è previsto che egli comunque possa delegare i suoi poteri in materia di *cyber security* all'Autorità delegata per la sicurezza della Repubblica [47].

A supporto delle attività della Presidenza del Consiglio, il d.l. n. 82/2021 prevede l'istituzione di un apposito Comitato interministeriale per la cybersicurezza (CIC), «con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza» [48]. La composizione del CIC ben rappresenta l'ampiezza e la trasversalità di tali politiche: oltre al Presidente del Consiglio, infatti, è prevista la partecipazione dei Ministri degli affari esteri, dell'interno, della giustizia, della difesa, dell'economia, dello sviluppo economico (oggi delle imprese), della transizione ecologica (oggi dell'ambiente), dell'università, delle

---

Cybersecurity, indagini amministrative, cooperazione pubblico privata e processo penale. I rischi connessi ad un'era di diffusa prevenzione collaborativa, in questo volume.

[44] Sul punto, vedi ora la *Strategia nazionale di cybersicurezza 2022-2026*, con l'annesso *Piano di implementazione*, adottati dal Presidente del Consiglio con d.p.c.m. 17 maggio 2022, i quali individuano tre direttrici generali di azione (protezione degli *asset* strategici nazionali; risposta alle minacce, agli incidenti e alle crisi in ambiente *cyber*; sviluppo sicuro delle tecnologie digitali e della ricerca industriale), cui sono ricondotte ben 82 misure attuative (www.acn.gov.it).

[45] In questo senso, l'art. 2, comma 1, del d.l. n. 82/2021.

[46] Cfr. l'art. 2, comma 2, del d.l. n. 82/2021.

[47] Come previsto dall'art. 3 del d.l. n. 82/2021, in riferimento a quanto previsto dall'art. 3 della l. n. 124/2007.

[48] In particolare, il CIC «a) propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale; b) esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza; c) promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza; d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale» (art. 4, comma 2, del d.l. n. 82/2021).

infrastrutture, della transizione digitale (se istituito) [49].

Quanto all'ACN, essa è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, anche se «nei limiti di quanto previsto» dal d.l. stesso. Se, infatti, le elevate competenze tecniche richieste, unitamente alle esigenze di flessibilità nell'esercizio delle funzioni assegnate, sembrano richiamare il modello tradizionale di Agenzia, le esigenze di indirizzo e controllo politico relative a tale delicatissimo settore fanno emergere un evidente rapporto di strumentalità rispetto alle funzioni del Presidente del Consiglio in materia [50]. È, infatti, il Presidente del Consiglio, come abbiamo visto, a nominare i vertici dell'ACN, il cui Direttore generale è suo «diretto referente»; a determinare il fabbisogno finanziario annuo della stessa ACN [51]; ad esercitare la potestà regolamentare quanto all'organizzazione, al personale, alla contabilità e alla gestione delle procedure di appalto dell'ACN (in questi due ultimi casi, su proposta del Direttore generale) [52].

Quanto alle funzioni attribuite, appare evidente il fine del legislatore di individuare nell'ACN il fulcro dell'attuale architettura istituzionale in materia di cybersicurezza, anche attraverso il trasferimento in capo ad essa delle funzioni precedentemente riconosciute in materia ad una molteplicità di soggetti istituzionali differenti: Presidenza del Consiglio, DIS, Ministero dello sviluppo economico, Agenzia per l'Italia digitale (AgID). Si ratta di un complesso di

---

[49] Così l'art. 3, comma 3, del d.l. n. 82/2021, il cui successivo comma 5 stabilisce anche che «Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare».

[50] Il quale è previsto si avvalga dell'ACN per l'esercizio delle sue competenze in materia di cybersicurezza (art. 5, comma 2, d.l. n. 82/2021). Sul punto, si veda L. PARONA, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giornale di diritto amministrativo*, 2021, n. 6, p. 709 ss.

[51] In base a quanto previsto dall'art. 11, comma 1, del d.l. n. 82/2021.

[52] Sul punto, si vedano, rispettivamente gli artt. 6, commi 1 e 3; 12, commi 1 e 8; 11, comma 3; e 11, comma 4, del d.l. n. 82/2021. I relativi regolamenti sono stati adottati con i d.p.c.m. n. 223/2021, 224/2021, 222/2021 e 166/2022. Particolarmente significativa, sul punto, appare la previsione che il regolamento del personale e quello sulle procedure di appalto possano derogare alle disposizioni legislative vigenti, tenuto conte delle funzioni volte alla tutela della sicurezza nazionale nello spazio cibernetico. I regolamenti di organizzazione e di contabilità, a loro volta, sono adottati di concerto con il Ministro dell'economia. Per tutti i regolamenti in questione, poi, è prevista espressamente una procedura in deroga rispetto a quella prevista dall'art. 17 della l. n. 400/1988, con la conseguente esclusione del parere espresso dal Consiglio di Stato. In tutti i casi citati, comunque, deve essere sentito il CIC, è necessario il parere del Comitato parlamentare per la sicurezza della Repubblica (COPASIR), nonché (per il regolamento di organizzazione e per quello del personale) anche quello delle Commissioni parlamentari competenti per materia.

funzioni particolarmente ampio e articolato [53], che può tuttavia essere ricondotto a cinque grandi categorie: a) coordinamento tra i diversi soggetti coinvolti in materia di cybersicurezza, quale Autorità nazionale per la cybersicurezza; b) sviluppo di adeguate capacità preventive e di risposta efficace rispetto ad attacchi ed incidenti informatici; c) certificazione dei prodotti, dei processi e dei sistemi ICT, anche attraverso l'esercizio di poteri di vigilanza, di controllo e sanzionatori; d) cooperazione a livello europeo ed internazionale in materia di cybersicurezza; e) supporto alla ricerca, all'innovazione tecnologica e allo sviluppo delle competenze in materia di cybersicurezza.

In via generale, l'ACN è espressamente definita quale «Autorità nazionale per la cybersicurezza» e, in tale veste, «assicura […] il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove 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» [54]. In questa veste, tra l'altro, predispone la già citata strategia nazionale di cybersicurezza, adottata dal Presidente del Consiglio dei ministri, che ben identifica il ruolo strategico dell'ACN, che deve coordinarsi con le altre Amministrazioni coinvolte in materia: il Ministero dell'interno [55], con particolare riferimento alle forze di polizia e al Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) della Polizia di Stato [56], il Ministero della difesa, con particolare riferimento alla difesa

[53] Cfr., in particolare, l'art. 7 del d.l. n. 82/2021. Sul punto, vedi ora anche quanto previsto dall'art. 20 della l. n. 132/2025, in base alla quale ACN e AgID sono designate Autorità nazionali per l'intelligenza artificiale. In particolare, all'ACN, «anche ai fini di assicurare la tutela della cybersicurezza», è affidata la responsabilità di vigilare sui sistemi di intelligenza artificiale, con i connessi poteri ispettivi e sanzionatori, secondo quanto previsto dalla normativa nazionale e da quella dell'UE. L'ACN, inoltre, è responsabile «per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza». Infine, è previsto che entrambe le Agenzie (ciascuna per quanto di competenza) assicurino «l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiali» conformi alla già citata normativa, assicurando al contempo il coordinamento e la collaborazione con le pubbliche amministrazioni e le autorità indipendenti coinvolte.

[54] Così l'art. 7, comma 1, lett. a) del d.l. n. 82/2021.

[55] Di cui vengono espressamente mantenute ferme le attribuzioni in quanto Autorità nazionale di pubblica sicurezza: art. 7, comma 1, lett. a), del d.l. n. 82/2021.

[56] Cfr. l'art. 7-*bis* del d.l. n. 144/2005, in base al quale, il CNAIPIC è l'organo del Ministero dell'interno deputato a garantire «la sicurezza e […] la regolarità dei servizi di telecomunicazione», assicurando «i servizi di protezione informatica delle infrastrutture critiche informatizzate di

cibernetica e al ruolo del Comando delle operazioni in rete (COR) [57]; il Sistema di informazione per la sicurezza della Repubblica, per quanto riguarda la ricerca ed elaborazione informativa in ambiente *cyber* coordinata dal DIS e svolta dalle due Agenzie (AISE ed AISI) [58]; il Ministero degli esteri, in relazione alla cooperazione internazionale in materia di cybersicurezza [59].

Quanto alla garanzia di sicurezza delle reti e dei sistemi informativi e alle misure preventive e di risposta in caso di incidenti informatici, l'ACN è ora individuata come "Autorità nazionale competente e punto di contatto unico" per le finalità di cui alla già citata normativa NIS [60]; parallelamente, come già accennato, il d.l. n. 82/2021 ha previsto il trasferimento in capo all'Agenzia delle competenze della Presidenza del Consiglio, del DIS e del Ministero dello sviluppo economico in materia di PSNC, con gli annessi poteri di vigilanza, controllo e sanzione [61]. Coerentemente con tale scelta, sono stati trasferiti presso l'ACN sia il già citato Centro di valutazione e certificazione nazionale (CVCN) [62] sia il CSIRT nazionale, con particolare riferimento ai menzionati obblighi di notifica degli incidenti informatici [63]. Da ultimo, l'Agenzia

interesse nazionale» individuate con decreto dello stesso Ministero dell'interno (vedi il d.m. 9 gennaio 2008). Sul punto, si veda G. TROMBETTA, *Ministero dell'interno e cybersecurity*, in R. Ursi, *op. cit.*, p. 85 ss.

[57] Istituito il 9 marzo del 2020 alle dipendenze del Capo di Sato Maggiore della Difesa, il COR è responsabile della condotta delle operazioni nel dominio cibernetico, nonché della gestione tecnico-operativa in sicurezza di tutti i sistemi ICT della Difesa.

[58] Ferme restando le competenze del comparto *intelligence* in materia di reti, sistemi informativi e servizi informatici attinenti alla gestione delle informazioni classificate, sulla base di quanto previsto dalla l. n. 124/2007 e dai successivi regolamenti di attuazione (cfr. l'art. 7, comma 1, lett. a), del d.l. n. 82/2021).

[59] Cfr. l'art. 7, comma 1, lett. q) del d.l. n. 82/2021.

[60] In questo senso, vedi l'art. 7, comma 1, lett. d) del d.l. n. 82/2021. Sul punto, vedi anche quanto disposto dalle successive lett. n), n-*bis*), in base alle quale l'ACN «sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT […]. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità» e «svolge ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici» (così il testo risultante dalle modifiche introdotte dal d.l. n. 105/2023).

[61] Si veda, in particolare, l'art. 7, comma 1, lett. f), h), i) del d.l. n. 82/2021.

[62] In questo senso l'art. 7, comma 4, del d.l. n. 82/2021.

[63] Cfr. l'art. 7, comma 1, lett. d-*ter*) del d.l. n. 82/2021. Sulla base di tali informazioni, l'ACN "provvede alla raccolta, all'elaborazione e alla classificazione" dei relativi dati, "che sono resi pubblici" nell'ambito della sua relazione annuale (art. 7, comma 1, lett. n-*ter*) del d.l. n. 82/2021).

partecipa alle esercitazioni nazionali ed internazionali riguardanti la simulazione di eventi di natura cibernetica [64].

All'ACN, poi, sono attribuiti importanti compiti di certificazione, essendo individuata quale Autorità nazionale di certificazione ai sensi del già citato Regolamento (UE) n. 2019/881 (c.d. *Cybersecurity Act*) ed assumendo «tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico», comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle prescritte sanzioni [65].

Sul piano della cooperazione sovranazionale, con particolare riferimento all'UE, l'ACN risulta a pieno titolo inserita nella rete europea delle corrispondenti Autorità nazionali NIS, in un continuo confronto con l'ENISA volto al complessivo rafforzamento del livello di cybersicurezza comune europeo. In quest'ottica, l'Agenzia è tenuta a cooperare anche con la già citata rete di CSIRT europei. Più in generale, è previsto che essa possa stipulare accordi «con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza […], ferme restando le competenze del Ministero degli affari esteri», anche mediante il coinvolgimento del settore privato e industriale [66]. Da ultimo, «promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali […], ferme restando le competenze del Ministero degli affari esteri» e garantendo il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza [67].

Infine, quanto alla promozione della ricerca e all'innovazione tecnologica l'ACN «supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore». Sempre in quest'ottica, l'ACN «promuove la formazione […] nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di

---

[64] Sulla base di quanto stabilito dall'art. 7, comma 1, lett. o) del d.l. n. 82/2021, al fine di «innalzare la resilienza del paese».

[65] Cfr. l'art. 7, comma 1, lett. e) del d.l. n. 82/2021. Sul punto, cfr. G.G. CUSENZA, *I poteri dell'Agenzia per la cybersicurezza nazionale: una nuova regolazione del mercato cibernetico*, in R. Ursi, *op. cit.*, p. 123 ss.

[66] In questo senso l'art. 7, comma 1, lett. s) del d.l. n. 82/2021.

[67] Secondo quanto previsto dall'art. 7, comma 1, lett. t) del d.l. n. 82/2021.

apposite convenzioni con soggetti pubblici e privati» [68].

Un fascio di competenze, dunque, molto ampio, e che vede nell'Agenzia uno snodo essenziale dell'attuale governo nazionale della cybersicurezza. Tale ruolo strategico, ancora una volta, è confermato anche dalla previsione (quasi una norma di chiusura) in base alla quale l'ACN «cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale», esprimendo «pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza» [69]. In questo modo, anche alla luce delle sue elevate competenze tecniche, l'ACN è individuata quale interlocutrice privilegiata del decisore politico quanto alla necessaria opera di aggiornamento e revisione della (complessa) normativa di settore.

Pur essendo finalizzato, come già anticipato, ad un superamento del precedente assetto che vedeva le competenze in materia di *cyber security* attratte al comparto *intelligence*, il d.l. n. 82/2021 ci consegna un assetto istituzionale che, inevitabilmente, rimane ancora in parte collegato al Sistema di informazione per la sicurezza della Repubblica [70]. Diversi, sul punto, appaiono i dati rilevanti. In primo luogo, come abbiamo visto, viene confermato il ruolo centrale della Presidenza del Consiglio dei ministri, la quale riveste quindi contemporaneamente il ruolo di «alta direzione» delle politiche di cybersicurezza e di Autorità nazionale per la sicurezza della Repubblica. Tale circostanza è plasticamente confermata anche nella scelta di prevedere, quale eventuale Autorità delegata in materia di cybersicurezza, l'Autorità delegata per la sicurezza della Repubblica.

D'altronde, vengono mantenuti inalterati alcuni rilevanti poteri del Presidente del Consiglio in materia di cybersicurezza anche nell'ambito delle sue funzioni di Autorità nazionale per la sicurezza della Repubblica. Particolarmente evidente, sul punto, è l'art. 5 del d.l. n. 105/2019, in base al quale egli,

---

[68] Da ultimo, vedi l'*Agenda di ricerca e innovazione per la cybersicurezza 2023-2026*, elaborata d'intesa con il Ministero dell'università e della ricerca (www.acn.gov.it). Particolarmente significativa, in questo senso, appare anche l'istituzione presso l'ACN del Centro nazionale di crittografia, nell'ambito delle attività di rafforzamento dell'autonomia industriale e tecnologica del paese, in collaborazione con centri universitari e di ricerca, al fine di conseguire nuove capacità crittografiche, secondo quanto previsto dall'art. 7, comma 1, lett. m-*bis*) del d.l. n. 82/2021 (ferme restando, in ogni caso, le competenze dell'Ufficio centrale per la segretezza nell'ambito delle materie sottoposte a classifica per motivi di sicurezza nazionale (art. 9, l. n. 124/2007).

[69] Così l'art. l'art. 7, comma 1, lett. p) del d.l. n. 82/2021.

[70] Cfr., in questo senso, A. Renzi, *La sicurezza cibernetica: lo stato dell'arte*, in *Giornale di diritto amministrativo*, 2021, n. 4, p. 538 ss.; S. Rossa, *Cybersicurezza e pubblica amministrazione*, Napoli, Editoriale Scientifica, Napoli, 2023, in particolare p. 91 ss.

«in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, può […] disporre, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, in deroga ad ogni disposizione vigente, nel rispetto dei principi generali dell'ordinamento giuridico e secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati» [71].

Da ultimo, vedi anche quanto previsto dall'art. 7-*ter* del d.l. n. 144/2005, introdotto dall'art. d.l. n. 115/2022, in relazione alle misure di *intelligence* di contrasto attivo in ambito cibernetico, in base al quale lo stesso Presidente del Consiglio emana specifiche disposizioni per fronteggiare «situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale». Tali disposizioni, in particolare, «disciplinano il procedimento di autorizzazione, le caratteristiche e i contenuti generali delle misure che possono essere autorizzate in rapporto al rischio per gli interessi nazionali coinvolti, secondo criteri di necessità e proporzionalità», prevedendo che dell'attuazione di tali misure siano incaricate le Agenzie di *intelligence*.

A conferma di tali (inevitabili) legami, può essere segnalata la composizione del Nucleo per la cybersicurezza (NC), istituito ora presso l'Agenzia, quale organo di supporto operativo del Presidente del Consiglio nell'ambito della prevenzione e preparazione rispetto ad eventuali situazioni di crisi cibernetica [72]. Il

---

[71] Secondo quanto previsto dalla disposizione in questione, «laddove nelle determinazioni di cui al presente comma sia recata deroga alle leggi vigenti anche ai fini delle ulteriori necessarie misure correlate alla disattivazione o all'interruzione, le stesse determinazioni devono contenere l'indicazione delle principali norme a cui si intende derogare e tali deroghe devono essere specificamente motivate» (in questo senso l'art. 5 del d.l. n. 105/2019, così come modificato dal d.l. n. 21/2022). In relazione a tale ipotesi, spetta poi all'ACN provvedere «sulla base delle attività di competenza del Nucleo per la cybersicurezza […] alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio» (art. 7, comma 1, lett. l), del d.l. n. 87/2021).

[72] Cfr. gli artt. 8 ss. del d.l. n. 82/2021. Tale organismo va sostituire il Nucleo per la sicurezza cibernetica (NSC), previsto fin dal d.p.c.m. 24 gennaio 2013 (oltre che da successivo d.p.c.m. 17 febbraio 2017), istituito prima presso l'Ufficio del Consigliere militare della Presidenza del Consiglio, e successivamente incardinato presso il DIS. Sempre a tali d.p.c.m. si deve, in generale, una definizione di crisi cibernetica quale «situazione in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria» (così l'art. 2). Sul punto, si veda F. SERINI, *op. cit.*, p. 265 ss.

NC, presieduto dal Direttore generale dell'ACN, è composto dal Consigliere militare del Presidente del Consiglio, da rappresentanti del DIS e delle Agenzie di intelligence (AISE ed AISI), oltre che da un rappresentante per ciascuno dei Ministeri coinvolti nel CIC e del Dipartimento della protezione civile [73]. In ogni caso, il NC può sempre essere convocato in composizione ristretta, con la sola partecipazione delle amministrazioni e dei soggetti via via interessati [74]. Il NC, in questo caso, svolge il ruolo di raccordo operativo, e per questo motivo acquisisce, tramite il CSIRT, tutte le comunicazioni relative ad incidenti informatici, valutando se essi «assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale, provvedendo in tal caso a informare tempestivamente il Presidente del Consiglio dei ministri» [75].

Da ultimo, un'ulteriore conferma sembra venire dalla recente riforma della composizione dello stesso Comitato interministeriale per la sicurezza della Repubblica (CISR), attuata dalla l. n. 90/2024 [76]. Infatti, con l'aggiunta del Ministri dell'agricoltura, delle infrastrutture e dell'università, la sua attuale composizione è stata sostanzialmente allineata a quella del già citato Comitato interministeriale per la cybersicurezza (CIC), salvo alcune piccole differenze [77].

---

[73] Si veda quanto previsto dall'art. 8, comma 2, del d.l. n. 82/2021. Tuttavia, di fronte a crisi di natura cibernetica, il NC è integrato (a seconda delle necessità) da un rappresentante del Ministero della salute e del Dipartimento dei Vigili del fuoco. In questo caso, inoltre, alle riunioni «possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, e di altri soggetti pubblici o privati eventualmente interessati» (art. 10, comma 3, del d.l. n. 82/2021).

[74] In questo senso l'art. 8, comma 4, del d.l. n. 82/2021. Tuttavia, in relazione a «specifiche questioni di particolare rilevanza», tale composizione ristretta può essere «di volta in volta estesa» ad un rappresentante della Direzione nazionale antimafia e antiterrorismo, della Banca d'Italia o di uno o più soggetti ricompresi nel PSNC, nonché di eventuali altri soggetti interessati (art. 8, comma 4.1, del d.l. n. 82/2021).

[75] Cfr. l'art. 9, comma 1, lett. f), g), del d.l. n. 82/2021. Una particolare attenzione è data ai «casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi» riguardanti il comparto *intelligence*, le forze di polizia, le strutture della Difesa e le altre amministrazioni coinvolte nel NC (art. 9, comma 1, lett. e), del d.l. n. 82/2021).

[76] Cfr. l'art. 7 della l. n. 90/2024.

[77] Il Ministro dell'agricoltura, infatti, non è componente del CIC, mentre il Ministro dell'innovazione tecnologica (se istituito) non è componente del CISR.

4. La governance della cybersicurezza: problemi e prospettive di un sistema integrato e multilivello

Dunque, un quadro istituzionale particolarmente variegato e complesso, sia in relazione alle fonti normative che la disciplinano [78], sia in relazione ai soggetti che ne sono i protagonisti [79]. Si tratta, come abbiamo visto, di un sistema che non solo coinvolge diverse amministrazioni dello Stato e operatori economici privati, ma risulta anche articolato su più livelli, con particolare riferimento alla dimensione europea e internazionale. Così, in ogni caso, non potrebbe non essere, rappresentando la trasformazione digitale uno degli obiettivi strategici non solo dell'UE, ma anche dei singoli Stati.

Alla luce della sua natura strategica e trasversale, non stupisce che la responsabilità politica venga affidata alla Presidenza del Consiglio dei ministri, nell'ambito della sua tradizionale funzione di direzione della politica generale del Governo, *ex* art. 95 Cost. Tuttavia, si tratta di un ambito che richiede elevate competenze di natura tecnica, capacità di coordinamento e rapidità di intervento, anche alla luce dell'aumento esponenziale del rischio e delle minacce in ambiente *cyber* cui si è assistito negli ultimi anni, anche attraverso l'utilizzo di veri e propri strumenti di natura ibrida [80].

La Presidenza del Consiglio, tuttavia, sembra giocare un ruolo a geometria variabile, inserendosi in moduli procedimentali a collegialità più o meno estesa all'interno del Governo. Se, infatti, le nomine del Direttore generale e del Vice-Direttore è previsto avvengano previa deliberazione del Consiglio dei ministri, quest'ultimo non risulta successivamente coinvolto in nessuna altra scelta strategica in materia di *cyber security*.

Tuttavia, si assiste ad un recupero di (pur parziale) collegialità grazie alle rilevanti attribuzioni del già citato Comitato interministeriale per la cybersicurezza (CIC) il quale, nell'ambito delle sue funzioni di consulenza, proposta e

---

[78] In relazione alle quali sarebbe auspicabile un'opera di riordino e di semplificazione. Per la recente proposta di adottare un codice in materia di cybersicurezza, vedi ora E. LONGO, *Il diritto costituzionale e la cybersicurezza*, cit., p. 344.

[79] Sul punto, tra gli altri, A. LAURO, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *Rivista Gruppo di Pisa*, 2021, n. 3, p. 529 ss.; F. GAGGERO, *L'azione normativa del Governo in materia di cybersecurity*, in F. BAILO-M. FRANCAVIGLIA (a cura di), *Bilanci e prospettive attorno ai poteri del Governo*, Napoli, Jovene, 2023, p. 347 ss.; F. SANCHINI, *Sicurezza cibernetica e architettura istituzionale: verso una governance costituzionalmente orientata?*, in *Federalismi.it*, 2025, n. 26, p. 170 ss.

[80] Si pensi, solo per fare un esempio, all'utilizzo sempre più evidente di *fake news* nell'ambito di vere e proprie campagne strategiche di disinformazione, attraverso l'utilizzo della rete e dei *social networks*, al fine di inquinare il dibattito pubblico e di influenzare le dinamiche democratiche interne.

vigilanza, (tra l'altro) propone gli indirizzi generali delle politiche di cybersicurezza e vigila sull'attuazione della strategia nazionale in materia [81]. Il Comitato, inoltre, deve essere sentito prima dell'adozione dei diversi d.p.c.m. attuativi previsti dal d.l. n. 82/2021 [82], oltre che proporre alcuni dei più importanti regolamenti previsti dal d.l. n. 105/2019, in materia di Perimetro di sicurezza nazionale cibernetica (PSNC) [83]. Sempre in relazione al PSNC, il Comitato ha il compito di proporre al Presidente del Consiglio il già citato provvedimento amministrativo (segretato) che individua i soggetti rientranti all'interno del Perimetro stesso, oltre che i relativi aggiornamenti [84]. Il CIC, infine, deve esprimere il proprio parere anche sul bilancio preventivo e consuntivo adottati ogni anno dal Direttore generale e approvati con d.p.c.m. [85].

Tuttavia, di fronte a situazioni di crisi che coinvolgono aspetti di cybersicurezza rilevanti per la sicurezza nazionale, qualora il Presidente del Consiglio decida, invece, di convocare il Comitato interministeriale per la sicurezza della Repubblica (CISR), è previsto che alle sedute debba partecipare anche il Direttore generale dell'ACN [86]. Ogni volta che il Presidente del Consiglio attivi il comparto *intelligence*, però, emergono tutti i tratti di "ministerialità" che caratterizzano da sempre le sue rilevanti competenze in materia di sicurezza nazionale, e le forme di (parziale) collegialità risultano conseguentemente più limitate. Si vedano, ad esempio, i già citati casi del potere di disattivazione di apparati o prodotti informatici impiegati nelle reti «in presenza di un rischio grave e imminente per la sicurezza nazionale», che pure avviene previa deliberazione del CISR (*ex* art. 5, d.l. n. 105/2019); o dell'autorizzazione di specifiche misure di *intelligence* di contrasto in ambito cibernetico «in situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale», per le quali deve comunque essere acquisito il parere del CISR (*ex* art. 7-*ter* del d.l. n. 174/2015) [87].

---

[81] Particolarmente significativo, in questo senso, appare il fatto che le funzioni di Segretario del CIC sono svolte dallo stesso Direttore generale dell'ACN (cfr. l'art. 4, comma 4, del d.l. n. 82/2021).

[82] Con particolare riferimento ai già citati regolamenti di organizzazione interna, del personale, di contabilità e sulle procedure di appalto dell'ACN.

[83] Tale previsione, a ben vedere, è la conseguenza diretta delle modifiche di cui al d.l. n. 82/2021, il cui art. 4, comma 6, prevede che il CIC «svolge […] le funzioni già attribuite al Comitato interministeriale per la sicurezza della Repubblica (CISR)» dal d.l. n. 105/2019, «fatta eccezione per quelle previste dall'art. 5» del medesimo d.l.

[84] Cfr. l'art. 1, comma 2-*bis*, del d.l. n. 105/2019.

[85] Come previsto dall'art. 11, comma 3, lett. a), del d.l. n. 82/2021, il quale prevede anche che debbano essere successivamente trasmessi alla Corte di conti.

[86] In questo senso l'art. 10, comma 1, del d.l. n. 82/2021, il quale prevede anche la partecipazione del Ministro dell'innovazione tecnologica, se istituito.

[87] Significativo, in quest'ultimo caso, l'espresso rinvio alle disposizioni in materia di garanzie funzionali degli addetti ai Servizi di informazione (artt. 17 ss. della l. n. 124/2007).

Tale assetto, più in generale, risulta confermato anche dal ruolo sostanzialmente strumentale assunto dall'ACN in relazione alle competenze della Presidenza del Consiglio in materia di cybersicurezza.

Proprio per questo, l'attuale architettura istituzionale prevede specifiche forme di controllo parlamentare [88], le quali tuttavia vengono rimesse, per lo più, al già citato Comitato parlamentare per la sicurezza della Repubblica (COPASIR), tradizionalmente competente a vigilare sull'attività dei servizi di informazione e sulla gestione del segreto di Stato da parte della Presidenza del Consiglio dei ministri.

È, infatti, a tale Comitato, ad esempio, che il Presidente del Consiglio deve comunicare non solo il più volte citato provvedimento amministrativo (ed i successivi aggiornamenti) con cui vengono individuati i soggetti inclusi nel PSNC [89], ma anche (e preventivamente) le nomine del Direttore generale e del Vice-Direttore dell'ACN (in questo ultimo caso tale comunicazione deve essere fatta anche alle Commissioni parlamentari competenti) [90]. Parallelamente, il COPASIR può chiedere l'audizione del Direttore generale stesso «su questioni di propria competenza», ai sensi dell'art. 31, comma 3, della l. n. 124/2007 [91].

Sempre in relazione ad aspetti significativi dell'organizzazione interna e delle attività dell'Agenzia, è previsto che il COPASIR debba esprimere un parere sui regolamenti di organizzazione, del personale, di contabilità e sulle procedure di appalto dell'ACN; sui primi due, in aggiunta, è prevista anche l'acquisizione del parere «delle Commissioni parlamentari competenti per materia e per i profili finanziari». Uno schema sostanzialmente analogo è previsto in relazione ad alcuni dei d.p.c.m. attuativi del PSNC, che devono essere trasmessi non solo al COPASIR, ma anche alle Commissioni parlamentari competenti per materia, le quali devono esprimere il proprio parere [92].

---

[88] Sul punto, si veda O. CARAMASCHI, *La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari*, in *Osservatorio costituzionale AIC*, 2022, n. 4, p. 69 ss.

[89] Cfr. l'art. 1, comma 4-*ter*, del d.l. n. 105/2019, il quale prevede che tale comunicazione debba avvenire «entro dieci giorni dall'adozione».

[90] Come previsto dall'art. 2, comma 3, del d.l. n. 82/2021. Quanto al personale, il successivo art. 12, comma 5, stabilisce che «dei provvedimenti adottati in materia di dotazione organica dell'Agenzia è data tempestiva e motivata comunicazione alla Commissioni parlamentari competenti e al COPASIR».

[91] Cfr. l'art. 5, comma 6, del d.l. n. 82/2021. Particolarmente significativo, in questo caso, il riferimento alla disposizione della l. n. 124/2007 che stabilisce che il COPASIR «può […] ascoltare ogni altra persona non appartenente al Sistema di informazione per la sicurezza in grado di fornire elementi di informazione o di valutazione ritenuti utili ai fini dell'esercizio del controllo parlamentare», quasi a voler ribadire (ancora una volta) la collocazione dell'ACN al di fuori del comparto *intelligence*.

[92] Secondo quanto previsto dall'art. 1, comma 4-*bis*, del d.l. n. 105/2019, con particolare

Ulteriore profilo, particolarmente delicato, attiene alla gestione del bilancio interno dell'ACN la quale, come abbiamo già visto, gode (tra l'altro) di autonomia contabile e finanziaria. Il d.l. n. 82/2021, infatti, prevede non solo che il Presidente del Consiglio debba previamente comunicare al COPASIR lo stanziamento annuale di risorse assegnate all'ACN [93], ma anche che debba essergli trasmesso (oltre che alle Commissioni parlamentari competenti) il bilancio consuntivo dell'Agenzia, unitamente alla relazione della Corte dei conti [94].

Quanto ai più generali obblighi di comunicazione al Parlamento, è previsto che il Presidente del Consiglio debba trasmettere annualmente alle Camere una Relazione sull'attività svolta dall'ACN nell'anno precedente [95]. Parallelamente, è previsto l'invio, da parte dello stesso Presidente del Consiglio, di un'altra relazione, questa volta diretta al COPASIR, ma relativamente «agli ambiti concernenti la tutela della sicurezza nazionale nella spazio cibernetico» [96].

Da ultimo, anche l'esercizio dei poteri del Presidente del Consiglio in materia di cybersicurezza più strettamente connessi con la tutela della sicurezza nazionale, e coinvolgenti quindi il comparto *intelligence*, prevede la necessità di un controllo da parte del COPASIR. Infatti, sia i provvedimenti di disattivazione, di cui all'art. 5 del d.l. n. 109/2015, sia le misure di contrasto in ambito cibernetico, di cui all'art. 7-*ter* del d.l. n. 174/2015, devono essere comunicati, rispettivamente, entro trenta giorni dalla loro adozione o dalla data di conclusione delle relative operazioni [97].

In conseguenza di tali previsioni, l'attenzione del COPASIR alla cybersicurezza è andata progressivamente aumentando negli ultimi anni, come dimostrato anche dall'esame delle Relazioni periodiche approvate nelle ultime legislature,

---

riferimento ai già citati d.p.c.m. n. 131/2020, sui criteri generali di individuazione dei soggetti inclusi nel PSNC, e d.p.c.m. n. 81/2021, in materia di notifica degli incidenti informatici rilevanti.

[93] Come stabilito dall'art. 11, comma 1, del d.l. n. 82/2021.

[94] Cfr. l'art. 11, comma 3, lett. b) del d.l. n. 82/2021.

[95] Il termine previsto è quello del 30 aprile di ogni anno (cfr. l'art. 14, comma 1, del d.l. n. 82/2021). Da ultimo, vedi la già citata *Relazione* per le attività svolte nel 2024 (Doc. CCXVIII, n. 4; presentata il 5 maggio 2025), www.acn.gov.it; www.parlamento.it.

[96] In questo senso l'art. 14, comma 2, del d.l. n. 82/2021, il quale prevede come termine di presentazione il 30 giugno di ogni anno.

[97] Cfr. quanto previsto dall'art. 5, comma 1-*bis*, del d.l. n. 109/2019 e dall'art. 7-*ter*, comma 4, del d.l. n. 174/2015 (che rinvia all'art. 33, comma 4, della l. n. 124/2007). Da ultimo, si segnala come, in occasione della Relazione del 2024, il COPASIR abbia confermato che, dall'entrata in vigore dell'ultima disposizione citata (introdotta dal già d.l. n. 115/2022), «non risultano essersi verificate le condizioni per l'attivazione di tali misure» (Doc. XXXIV, n. 3, p. 8) www.parlamento.it.

che ormai contengono una parte specificamente dedicata alla cybersicurezza [98]. Il COPASIR, parallelamente, ha deciso di svolgere anche alcuni approfondimenti in materia, attraverso lo svolgimento di apposite indagini conoscitive, indicando puntualmente la necessità di interventi normativi volti a rafforzare la sicurezza cibernetica nazionale, spesso accolti dal legislatore [99]. Da ultimo, alla luce dell'istituzione dell'ACN, il Comitato ha tuttavia segnalato la necessità di una maggiore definizione dei rapporti con il Sistema dei informazione per la sicurezza della Repubblica, anche per evitare possibili sovrapposizioni [100], le quali attualmente rischiano di manifestarsi anche sul piano della stessa attività di controllo parlamentare, vista la necessità di assicurare un coordinamento efficace tra il COPASIR e le Commissioni parlamentari permanenti competenti, più volte evocate.

Il tema, più in generale, richiede un'attenta riflessione in vista delle prospettive di riforma della *governance* in materia di sicurezza nazionale la quale, come abbiamo visto, ha subito forti sollecitazioni negli ultimi anni anche alla luce dell'evoluzione delle stesse minacce presenti nell'arena globale, che impongono un continuo aggiornamento dei protagonisti, delle politiche, degli assetti e delle concrete azioni operative. In questo senso, da ultimo, si riaffaccia l'annosa questione dell'istituzione, nell'ordinamento italiano, di un vero e proprio Consiglio di sicurezza nazionale, che potrebbe rappresentare il fulcro di elaborazione delle politiche e delle azioni a tutela della sicurezza nazionale e degli interessi strategici del paese, direttamente collegato alla Presidenza del Consiglio dei ministri, e la cui introduzione porterebbe non solo ad una complessiva rivisitazione degli attuali Comitati interministeriali competenti in materia (CISR e CIC), ma anche ad un parziale ripensamento del ruolo dello stesso Consiglio

---

[98] Si vedano, in particolare, la Relazione del 2017, approvata sul finire della XVII Legislatura (Doc. XXXIV, n. 5), tutte le Relazioni approvate nel corso della XVIII Legislatura (Doc. XXXIV, nn. 4, 8 e 12), nonché le Relazioni del 2023 e del 2024, approvate nella XIX Legislatura, attualmente in corso (Doc. XXXIV, nn. 1 e 3) www.parlamento.it.

[99] In questo senso, in particolare, si ricordano la *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, approvata il 7 luglio 2010 (XVI Legislatura, Doc. XXXIV, n. 4) nonché, da ultimo, la *Relazione sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale*, approvata l'11 dicembre 2019 (XVIII Legislatura, Doc. XXXIV, n. 1), www.parlamento.it.

[100] Cfr., in particolare, la *Relazione sull'attività svolta dal 1° gennaio 2021 al 9 febbraio 2022*, secondo la quale, alla luce della natura sempre più ibrida che le minacce alla scurezza nazionale stanno assumendo nell'attuale scenario, «appare opportuna una rivisitazione della l. n. 124/2007 per una armonizzazione e una più lineare definizione di perimetri e competenze dei diversi soggetti coinvolti nella tutela della sicurezza nazionale nel dominio cibernetico e delle relative funzioni di controllo che il Comitato parlamentare per la sicurezza della Repubblica è chiamato a svolgere» (XVIII Legislatura, Doc. XXXIV, n. 8, p. 42), www.parlamento.it.

supremo di difesa (CSD), presieduto dal Capo dello Stato.

In attesa di tali problematici orizzonti, almeno quanto alla cybersicurezza, è senza dubbio sul piano della capacità di svolgere un efficace ruolo di coordinamento della complessa architettura istituzionale in materia che si gioca gran parte del futuro dell'ACN, al crocevia tra coordinamento multilivello con l'UE e integrazione interna tra i diversi soggetti (pubblici e privati) coinvolti, a vario titolo, nel perimetro di sicurezza nazionale cibernetica [101]. Tra questi, come abbiamo visto, acquistano un ruolo fondamentale anche gli operatori economici nei settori considerati strategici, con i quali l'ACN dovrà promuovere adeguati strumenti di partenariato pubblico-privato, al fine di garantire non solo la sicurezza cibernetica nazionale, ma anche per rafforzare l'autonomia industriale, tecnologica e scientifica dell'Italia nel contesto europeo e internazionale [102].

[101] La necessità di una più stretta collaborazione delle amministrazioni pubbliche con l'Agenzia è stata ribadita dalla Direttiva del Presidente del Consiglio del 6 luglio 2023, con particolare riguardo alla gestione di incidenti di natura informatica. Sul punto, vedi anche quanto stabilito dall'art. 5, comma 5, del d.l. n. 82/2021, il quale prevede che l'ACN possa concludere accordi di collaborazione con «altri organi dello Stato» e «altre amministrazioni» per lo svolgimento dei suoi compiti istituzionali (si vedano ad esempio, i protocolli firmati nel 2023 con la Camera dei deputati e il Senato della Repubblica; per la collaborazione con il Garante per la protezione dei dati personali, in ogni caso, vedi anche l'art. 7, comma 5, del medesimo d.l.).

[102] Sul punto, appare particolarmente significativa la previsione in base alla quale l'ACN partecipa, «per gli ambiti di competenza», al Gruppo di coordinamento in merito all'esercizio dei poteri speciali da parte del Governo nell'ambito dei settori strategici (c.d. *golden power*); cfr. l'art. 7, comma 1, lett. g), del d.l. n. 82/2021.