ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

20 APRILE 2022

La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021

di Federico Serini
Dottorando di ricerca in Diritto pubblico, comparato e internazionale
Sapienza – Università di Roma

La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*

di Federico Serini
Dottorando di ricerca in Diritto pubblico, comparato e internazionale
Sapienza – Università di Roma

Abstract [It]: L'articolo propone una prima lettura del decreto-legge n. 82 del 14 giugno 2021, convertito, con modificazioni, in legge n. 109 del 4 agosto 2021, con il quale l'Italia ha aggiornato la *governance* di cybersicurezza nazionale. La riflessione, condotta alla luce del complesso quadro normativo recentemente realizzato sul tema, intende offrire una prima interpretazione sistematica di questa nuova branca della sicurezza all'interno del contesto normativo europeo e nazionale.

Title: The new cybersecurity governance in Italy: first reading notes to decree-law no. 82 of 2021
Abstract [En]: This article proposes a first reading of Decree-Law no. 82 of 14 June 2021, converted with amendments, into Law no. 109 of 4 August 2021, by which Italy has updated its national cyber security governance. The reflection, conducted in the light of the complex framework of regulations recently implemented on the subject, aims to offer a first systematic interpretation of this new branch of security within the European and national regulatory context.

Parole chiave: Cybersicurezza nazionale, Agenzia per la Cybersicurezza Nazionale (ACN), d.l. n. 82/2021, cyberawareness
Keywords: National cybersecurity; National Cybersecurity Agency; Decree-Law no. 82 of 14 June 2021; cyberawareness

1. Questioni introduttive sulle normative di cybersicurezza nel multilivello

Sebbene il diffuso utilizzo delle tecnologie informatiche sia stato portatore di indubbi benefici per le società e le economie, l'interoperabilità e l'interconnessione alla rete dei molti servizi, funzioni e infrastrutture necessarie alla vita dei consociati, ha avuto l'effetto di trasferire i pericoli del "cyberspazio" nel mondo reale, al punto che, come osservato da Alcuni, ormai «ogni società è tanto vulnerabile quanto è vulnerabile l'informatica di cui fa uso» e pertanto «più le società sono avanzate, più sono vulnerabili»[1].

* Articolo sottoposto a referaggio.
[1] M.G. LOSANO, *Guerre ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. FORNI - T. VETTOR (a cura di), *Sicurezza e libertà in tempi di terrorismo globale*, Torino, 2017, p. 22. Sugli effetti delle forme di connettività non solo dovute alle tecnologie ICT v. A.L. BARABÁSI, *Linked. How everything is connected to everything else and what it means for*

Si tratta infatti di una debolezza strutturale dovuta al fatto che la rete non è stata «concepita obbedendo a criteri di sicurezza ma, al contrario, *per garantire l'accesso e facilitare lo scambio di informazioni* [cors.d.A.]»[2]; condizione questa, che ha dato origine alla sempre più avvertita esigenza di rendere sicuro il "cyberspazio" al fine di garantire i diritti e le libertà nelle società moderne industrializzate[3].

Sul piano europeo e nazionale, gli interventi normativi sul punto sono stati declinati secondo le diverse componenti (o "*layers*") della rete[4], con l'intento di raggiungere adeguati livelli di sicurezza "nella" rete, vedi la proposta legislativa che prende il nome di "*Digital Services Act package*", volta ad aggiornare le norme che regolano i servizi digitali nell'Unione[5], e "della" rete, come le recenti normative emanate in tema di protezione delle reti, sistemi informativi e servizi informatici, emanate per far fronte ai crescenti attacchi informatici veicolati ai danni delle infrastrutture responsabili di funzioni e servizi essenziali per gli Stati[6].

È il caso delle due discipline su cui il decreto legge n. 82 del 14 giugno 2021 è andato - seppur in parte - ad apportare delle modifiche[7]. Si tratta della direttiva 2016/1148, anche nota come direttiva NIS (*Network*

business, science, and everyday life, New York, 2014. Analogamente v. anche P. KHANNA, *Connectography. Le mappe del futuro ordine mondiale*, Roma, 2016.

[2] G. CORASANITI, *Esperienza giuridica e sicurezza informatica*, Milano, 2003, p. 332.

[3] Sul concetto di sicurezza come diritto di libertà v. C. MOSCA, *La sicurezza come diritto di libertà*, Padova, 2012, ove l'A. con una audace interpretazione propone una chiave di lettura diversa di questo diritto, «capace di ricomprendere e non di escludere il tema della sicurezza dal novero dei diritti di libertà riconosciuti» (p. 45). In particolare, facendo riferimento a Calamandrei «in animo di superare l'antitesi tra il liberalismo che privilegia i diritti di libertà e il socialismo che esalta e antepone i diritti sociali», l'A. scrive che «per superare l'antitesi tra i diritti di libertà e diritto di sicurezza, basterebbe dichiarare quest'ultimo premessa indispensabile per assicurare la libertà, diventandone quasi contenuto oggettivo o invece – come si preferisce – sottolineare il diritto alla sicurezza come esso stesso diritto di libertà in ragione delle oggettive connessioni esistenti e richiamate in precedenza tra i diritti sociali e i diritti di libertà» (pp. 48-49). Sulla sicurezza in generale v. G. CERRINA FERONI – G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi costituzionali*, n. 1, 2008; T.F. GIUPPONI, *Le dimensioni costituzionali della sicurezza*, Bologna, 2010; G. COCCO (a cura di), *I diversi volti della sicurezza*, Milano, 2012; M. RUOTOLO, *Sicurezza, dignità e lotta alla povertà*, Napoli, 2012; L. FORNI - T. VETTOR (a cura di), *op. cit.*, 2017; F. PIZZOLATO – P. COSTA (a cura di), *Sicurezza e tecnologia*, Milano, 2017; A. STERPA, *Libertà dalla paura. Una lettura costituzionale della sicurezza*, Napoli, 2019; A. STERPA - A. COIANTE (a cura di), *Sicurezza, legalità ed economia*, Napoli, 2020; R. URSI, *La sicurezza pubblica*, Bologna, 2022.

[4] Cfr. C. MCTAGGART, *A layer approach to Internet legal analysis*, in *McGill Law Journal*, 2003, p. 571, (articolo consultabile sul sito del MCGILL LAW JOURNAL), ove l'A. individua tre "strati" del cyberspazio, ossia: il contenuto, lo strato più vicino all'utente costituito dalle applicazioni *software*; quello operativo, costituito dagli standard e protocolli che rendono possibile il funzionamento della rete; e infine, quello fisico, composto dall'insieme di macchinari, *hardware*, strumenti e reti attraverso i quali opera la rete.

[5] COM(2020) 842 del 15 dicembre 2020, "*Proposta di regolamento del parlamento europeo e del consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali)*".

[6] L'Associazione Italiana per la Sicurezza Informatica (CLUSIT), pubblica annualmente un rapporto con la collaborazione di esperti del settore e imprese, al fine di fornire una fotografia sugli eventi di sicurezza informatica che hanno interessato l'anno precedente. Nel report del 2021, l'Associazione ha registrato un sensibile aumento degli attacchi verso le infrastrutture critiche nell'arco di tempo dal 2014 al 2021 di circa l'85% in più rispetto all'anno precedente. Si precisa tuttavia, che la denuncia di simili criticità, legate all'impatto delle minacce cibernetiche non è attuale. Lo stesso trend caratterizza anche il report 2022, ove tra le diverse infrastrutture critiche si registrano picchi nel settore sanitario, dei trasporti, ricerca scientifica-tecnica, nonché settori strategici governativi come apparati militari e forze di polizia.

[7] Cfr. artt. 15 e 16 del decreto legge 14 giugno 2021, n. 82, ove sono state apportate modifiche alla disciplina NIS, a quella del PSNC. Tuttavia si precisa che le due disposizioni sono andate a modificare anche la l. 124/2007 recante disciplina sul "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", il d.l. n. 21/2012, recante disciplina su "Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza

and Information Security), finalizzata a realizzare un «livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno»[8], nonché, del decreto legge del 21 settembre 2019, n. 105, convertito con modificazioni in legge 18 novembre 2019, n. 133, con il quale l'Italia ha istituto il Perimetro Nazionale di Sicurezza Cibernetica (PSNC)[9] al fine di dettare una disciplina nazionale integrante quella europea attraverso il coinvolgimento nel PSNC di «tutti quegli operatori pubblici o privati, che, seppur non ricompresi nell'ambito di applicazione della Direttiva NIS, risultino comunque essenziali per la sicurezza nazionale italiana [...]»[10].

Si precisa tuttavia che la disciplina articolata nel d.l. n. 82/2021 si concentra perlopiù su un diverso profilo, che non attiene la protezione delle reti e delle risorse informatiche per motivi di sicurezza del mercato unico, o per motivi di sicurezza nazionale, ma interessa piuttosto lo sviluppo di un'idonea architettura istituzionale capace di far fronte alle minacce informatiche[11].

nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni", al c.d. Codice delle comunicazioni elettroniche, il d.lgs. n. 259/2003, la disciplina dell'Agenzia per l'Italia Digitale (AgID), ed infine il d.lgs. 104/2010 ove è stata conferita competenza per le controversie aventi ad oggetto i provvedimenti dell'Agenzia pe la Cybersicurezza Nazionale al T.A.R. del Lazio.

[8] art. 1, direttiva (UE) del 6 luglio 2016, n. 1148, "*recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione"* (c.d. direttiva NIS), recepita in Italia con il decreto legislativo 18 maggio 2018, n. 65.

[9] Il decreto legge del 21 settembre 2019, n. 105, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*", è stato convertito con modificazioni dalla l. 18 novembre 2019, n. 133. Si tratta tuttavia di un articolato programma la cui completa e concreta realizzazione è affidata ad una serie di regolamenti. Attualmente sono stati adottati il DPCM 30 luglio 2020, n. 131, che provvede a: definire le modalità e i criteri procedurali di individuazione dei soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel Perimetro di sicurezza nazionale cibernetica e che, pertanto, sono tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge 105/2019; definire i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica; il DPR 5 febbraio 2021, n. 54, che ha definito le procedure e modalità di valutazione delle acquisizioni da parte dei soggetti inclusi nel Perimetro di sicurezza cibernetica, di oggetti di fornitura le procedure delle attività di verifica e ispezione (art. 1, comma 6, DL 105/2019) e il DPR 14 aprile 2021, n. 81 che definisce le modalità per la notifica nel caso di incidenti riguardanti beni ITC (art. 1, comma 2, lett. b), DL 105/2019). Si prevede invece l'ulteriore attuazione di: un DPCM per definire le procedure di notifica degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici (art. 1, comma 3, DL 105/2019); e un DPCM che definisca i criteri per l'accreditamento di laboratori l'avvalimento di laboratori ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità. Con il medesimo DPCM sono stabiliti i raccordi tra il CVCN e i predetti laboratori, nonché tra il medesimo CVCN e i Centri di valutazione del Ministero dell'interno e del Ministero della difesa (art. 1, comma 7, DL 105/2019). Gli sviluppi del quadro normativo di cybersicurezza nazionale possono essere monitorati consultando la pagina dedicata alla documentazione parlamentare della Camera dei deputati.

[10] Cfr. S. MELE, *Il Perimetro di Sicurezza Nazionale Cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della pubblica amministrazione alla sicurezza nazionale*, in G. CASSANO – S. PREVITI (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020, p. 186. Nello specifico, confrontando le due citate discipline, la disciplina in questione si estende verso quei soggetti attivi nei settori interno, difesa, spazio e aerospazio, telecomunicazioni, economia e finanza, servizi digitali, tecnologie critiche.

[11] Cfr. A. COLELLA, *Analisi comparata delle architetture decisionali in materia di sicurezza cibernetica dei paesi dell'area euro-occidentale*, in A. TORRE, (a cura di), *Costituzioni e sicurezza dello Stato*, Santarcangelo di Romagna, 2013. V. inoltre, S. MELE, *I principi strategici delle politiche di cybersecurity*, 2013, (documento consultabile sul sito sicurezzanazionale.gov.it).

2. Il decreto-legge n. 82 del 14 giugno 2021

A pochi giorni dal noto attacco informatico contro il Centro Elaborazione Dati della Regione Lazio, il 3 agosto 2021 la Camera dei deputati e il Senato hanno convertito con modificazioni il decreto-legge n. 82 del 14 giugno 2021, in legge n. 109 del 4 agosto 2021.

Con tale intervento, dettato dalla condizione di «straordinaria necessità e urgenza» avvertita a livello nazionale in ossequio al crescente impatto degli attacchi informatici, nonché dalla priorità di garantire una sicura attuazione dei piani di trasformazione digitale recentemente delineati nel Piano Nazionale di Ripresa e Resilienza (PNRR)[12], si è inteso aggiornare la c.d. architettura nazionale di cybersicurezza, attraverso la creazione di un sistema istituzionale *ad hoc*.

La trattazione che segue è stata pertanto articolata secondo le tre principali aree di intervento del decreto, ossia la nuova architettura di cybersicurezza nazionale (2.1.); la creazione dell'Agenzia per la Cybersicurezza Nazionale – ANC (2.2.); le funzioni del Nucleo di Cybersicurezza – NC (2.3.), avendo modo di approfondire le peculiarità e gli aspetti innovativi di tali elementi nei rispettivi paragrafi.

2.1. L'architettura del sistema nazionale di cybersicurezza

I primi quattro articoli del decreto intervengono sul Sistema Nazionale di Sicurezza Cibernetica (SNSC), articolazione istituzionale che trova origine nel d.P.C.M. n. 66 del 19 marzo 2013 (decreto Monti), successivamente modificato con il d.P.C.M. n. 87 del 17 febbraio 2017 (decreto Gentiloni), ove si organizzava un'architettura sviluppata su tre livelli[13]. Il primo, quello politico, vedeva il Presidente del Consiglio dei ministri posto al vertice del sistema[14], supportato dal Comitato Interministeriale per la sicurezza della Repubblica (CISR), quale organo istituito con legge 3 agosto 2007, n. 124 presso la Presidenza del Consiglio dei Ministri, e avente funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza[15]. Il secondo livello, di carattere operativo e amministrativo, vedeva la partecipazione del Nucleo per la Sicurezza Cibernetica

[12] Il Piano Nazionale di Ripresa e Resilienza (PNRR) pone la "sicurezza cibernetica" a fondamento del processo di trasformazione digitale.

[13] Si precisa che il previgente sistema di cybersicurezza nazionale, istituito con il decreto Monti e poi modificato con il decreto Gentiloni, prevedeva anche altri organi deputati «*alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi*». Questi erano rispettivamente: l'Organismo di supporto al CISR, il Comitato scientifico e il NISP - Tavolo interministeriale di crisi cibernetica (i quali non vennero riconfermati quali componenti del sistema nel decreto Gentiloni), e infine, gli operatori privati «*che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici*» (di cui all'art. 11).

[14] Cfr. art. 3, d.P.C.M. n. 66 del 19 marzo 2013.

[15] Cfr. art. 4, d.P.C.M. n. 66 del 19 marzo 2013.

(NSC), istituito nell'ambito dell'Ufficio del Consigliere Militare presso la Presidenza del Consiglio dei Ministri, con la funzione di supportare il Presidente nella materia della sicurezza del "cyberspazio" per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento[16]. Infine, il terzo livello, composto dagli Organismi di informazione per la sicurezza, responsabili di condurre attività di ricerca informativa, nonché analisi, valutazioni e previsioni sulle minacce, ed alla trasmissione di informazioni rilevanti al Nucleo per la Sicurezza Cibernetica, e agli altri soggetti – sia pubblici che privati – interessati all'acquisizione di informazioni[17].

In considerazione di ciò, preme innanzitutto osservare che, diversamente dalla precedente organizzazione, con il decreto-legge n. 82/2021 si è inteso creare un'organizzazione non più afferente al Sistema di informazione per la sicurezza della Repubblica, ma un modello organizzativo separato e specializzato nel particolare settore della "sicurezza nel cyberspazio". Ne sono prova l'introduzione di due organi *ad hoc*, quali, il Comitato Interministeriale per la Cybersicurezza (CIC), l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), nonché la mancata conferma degli Organismi di informazione per la sicurezza tra gli attori componenti il nuovo SNSC.

Tuttavia, come si avrà modo di osservare in seguito, la nuova architettura, incardinata nella Presidenza del Consiglio dei ministri, continua ad essere legata alla medesima direzione operativa e strategica del Sistema di informazione per la sicurezza della Repubblica di cui alla l. 3 agosto 2007, n. 124.

L'attuale SNSC affida infatti al Presidente del Consiglio dei ministri – ovviamente confermandone la posizione di vertice del Sistema – compiti più estesi ed elevati rispetto a quelli assegnati nella previgente architettura. In particolare, richiamando la formulazione dell'art. 1 dell'appena citata l. n. 124 del 2007[18], l'art. 1, co. 1, lett. a) del decreto attribuisce in via esclusiva al Presidente «l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, anche ai fini della sicurezza nazionale nel cyberspazio»[19].

Le ulteriori attribuzioni, di cui alle lett. b) e c) del medesimo disposto, interessano invece l'adozione della strategia nazionale di cybersicurezza[20], sentito il Comitato Interministeriale per la Cybersicurezza (CIC),

---

[16] Cfr. artt. 8 e 9, d.P.C.M. n. 66 del 19 marzo 2013.

[17] Cfr. art. 7, d.P.C.M. n. 66 del 19 marzo 2013.

[18] Cfr. art. 1, co. 1, lett. a), legge 3 agosto 2007, n. 124, il quale prevede che al Presidente del Consiglio dei ministri sono attribuiti, in via esclusiva «l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento».

[19] Cfr. art. 3 del d.P.C.M. n. 66 del 19 marzo 2013 (decreto Monti), disponeva che il Presidente fosse responsabile dell'adozione del Quadro Strategico Nazione di Sicurezza Cibernetica (QSN), oltreché del Piano Nazionale (PN), conferendogli la possibilità di emanare direttive e «ogni atto d'indirizzo necessari per l'attuazione del Piano». L'art. 3 del d.P.C.M. n. 87 del 17 febbraio 2017 (decreto Gentiloni), riprendeva quanto previsto dal decreto Monti, precisando tuttavia al comma primo che il Presidente attua i programmi previsti nel disposto, «*quale responsabile della politica generale del Governo e vertice del Sistema di informazione per la sicurezza della Repubblica, ai fini della tutela della sicurezza nazionale anche nello spazio cibernetico*».

[20] Si tratta di un documento la cui stesura è contemplata all'art. 7 della direttiva NIS, rubricato "*Strategia nazionale in materia di sicurezza della rete e dei sistemi informativi*". Come precisato nell'Allegato 1 della Comunicazione della Commissione europea, "*Sfruttare al meglio le reti e i sistemi informativi – verso l'efficace attuazione della direttiva (UE) 2016/1148 recante misure per*

nonché la nomina e la revoca del direttore generale e del vicedirettore generale dell'Agenzia per la Cybersicurezza Nazionale (ACN), previa deliberazione del Consiglio dei ministri, e, ai sensi dell'art. 1, co. 3 del decreto, informando preventivamente di tali nomine il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), e le Commissioni parlamentari competenti.

Altra analogia con la direzione organizzativa del Sistema di informazione per la sicurezza della Repubblica è ravvisabile nell'introduzione dell'Autorità delegata di cui all'art. 3 del decreto[21]. Il disposto prevede che il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, possa delegare ad un Ministro senza portafoglio o ad un Sottosegretario di Stato[22], che prenderà il nome di "Autorità delegata", le funzioni attribuitegli in via non esclusiva dal decreto di cui all'art. 2. Tale Autorità è tenuta ad informare costantemente il Presidente del Consiglio sulle modalità di esercizio delle funzioni delegate, il quale, «fermo restando il potere di direttiva», può in qualsiasi momento avocare a sé l'esercizio di tutte o di alcune di esse, ed inoltre, in relazione alle funzioni delegate, partecipa alle riunioni del Comitato interministeriale per la transizione digitale (CITD)[23].

un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione", COM (2017)476 final del 4 ottobre 2017, tale strategia «è equiparabile alla "strategia nazionale di cybersicurezza" (NCSS)» (p. 5) (documento consultabile sul sito della Commissione europea). L'art. 6. co.1, del decreto legislativo 65/2018, con il quale l'Italia ha recepito la direttiva NIS, fa infatti riferimento alla NCSS, prevedendo al comma 2 che «nell'ambito della strategia nazionale di cybersicurezza, sono in particolare indicati, per la sicurezza di reti e sistemi informativi rientranti nell'ambito di applicazione del presente decreto: a) gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi informativi; b) il quadro di governance per conseguire gli obiettivi e le priorità, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; c) le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato; d) i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi; e) i piani di ricerca e sviluppo; f) un piano di valutazione dei rischi; g) l'elenco dei vari attori coinvolti nell'attuazione». Il co. 4 del decreto legislativo 65/2018, novellato a seguito dell'entrata in vigore del decreto-legge n. 82/2021, prevede inoltre che «l'Agenzia per la cybersicurezza trasmette la strategia nazionale in materia di cybersicurezza alla Commissione europea entro tre mesi dalla sua adozione. Può essere esclusa la trasmissione di elementi della strategia riguardanti la sicurezza nazionale».

[21] Cfr. art. 3 della l. 3 agosto 2007, n. 124, il quale prevede che «Il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare le funzioni che non sono ad esso attribuite in via esclusiva soltanto ad un Ministro senza portafoglio o ad un Sottosegretario di Stato, di seguito denominati "Autorità delegata". 2. L'Autorità delegata non può esercitare funzioni di governo ulteriori rispetto a quelle ad essa delegate dal Presidente del Consiglio dei ministri a norma della presente legge. 3. Il Presidente del Consiglio dei ministri è costantemente informato dall'Autorità delegata sulle modalità di esercizio delle funzioni delegate e, fermo restando il potere di direttiva, può in qualsiasi momento avocare l'esercizio di tutte o di alcune di esse. 4. In deroga a quanto previsto dal comma 1 dell'articolo 9 della legge 23 agosto 1988, n. 400, e successive modificazioni, non è richiesto il parere del Consiglio dei ministri per il conferimento delle deleghe di cui al presente articolo al Ministro senza portafoglio».

[22] Cfr. art. 3 della l. 3 agosto 2007, n. 124. Nel caso specifico, la delega è stata affidata con il d.P.C.M. 8 marzo 2021, al Sottosegretario di Stato Franco Gabrielli.

[23] Il CITD è organo istituito con il decreto-legge1 marzo 2021, n. 22, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 55, con il compito di assicurare «il coordinamento e il monitoraggio dell'attuazione delle iniziative di innovazione tecnologica e transizione digitale delle pubbliche amministrazioni competenti in via ordinaria». Sul punto, cfr. art. 8, co. 2, del decreto legge 1 marzo 2021, n. 22, convertito con modificazioni dalla legge 22 aprile 2021, n. 55, "*Disposizioni urgenti in materia di riordino delle attribuzioni dei Ministeri*".

I tratti innovativi della disciplina possono invece essere colti nella istituzione e introduzione nel nuovo assetto decisionale dei due già citati organi: il Comitato Interministeriale per la Cybersicurezza (CIC) e l'Agenzia per la Cybersicurezza Nazionale (ACN).

Relativamente al primo, il CIC è un organo politico istituito presso la Presidenza del Consiglio dei ministri, a cui l'art. 4 del decreto attribuisce le funzioni di «consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico»[24]. Si precisa, che il previgente Sistema assegnava tali funzioni al Comitato Interministeriale per la Sicurezza della Repubblica (CISR), il quale, sebbene ora non sia espressamente contemplato tra gli attori della nuova architettura di cybersicurezza nazionale, dall'art. 10 del d.l. n. 82/2021, emerge che l'Organo ne prenda parte ove convocato dal Presidente del Consiglio dei ministri nei casi di «crisi che coinvolgono aspetti di cybersicurezza»[25].

Al comma 2 del disposto sono poi specificate le funzioni attribuite al CIC di cui al comma 1 del decreto, attraverso l'assegnazione dei presenti compiti:

a) proposta al Presidente del Consiglio dei ministri degli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale;

b) esercizio dell'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza;

c) promozione dell'adozione di iniziative necessarie a 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 tal materia;

d) esprimere pareri sul bilancio preventivo e sul bilancio consuntivo dell'ACN.

Sebbene non contemplato dal disposto in esame, si evidenzia che il CIC esprime il suo parere, dietro richiesta del Presidente del Consiglio dei ministri, anche su «l'adozione della strategia nazionale di cybersicurezza», di cui all'art. 2, co. 1, lett. b) del decreto. Competenza questa che può essere dedotta dall'art. 4 comma 6 del decreto in commento, ove è espressamente previsto che il CIC si sostituisca al

[24] Cfr. art. 4, co. 1, del d.l. n. 82/2021.

[25] Cfr. art. 10 del d.l. n. 82/2021, ove al co. 1, prevede che «nelle situazioni di crisi che coinvolgono aspetti di cybersicurezza, nei casi in cui il Presidente del Consiglio dei ministri convochi il CISR in materia di gestione delle predette situazioni di crisi, alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'Agenzia», nonché, al co. 2, che «il Nucleo [per la Sicurezza Cibernetica] assicura il supporto al CISR e al Presidente del Consiglio dei ministri, nella materia della cybersicurezza, per gli aspetti relativi alla gestione di situazioni di crisi ai sensi del comma 1, nonché per l'esercizio dei poteri attribuiti al Presidente del Consiglio dei ministri, ivi comprese le attività istruttorie e le procedure di attivazione necessarie, ai sensi dell'articolo 5 del decreto-legge perimetro».

CISR nelle funzioni a questo attribuite dal decreto istitutivo del PSNC, «fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge perimetro»[26].

Il comma 3 dispone che al Comitato prendano parte: il Presidente del Consiglio dei Ministri, che lo presiede; l'Autorità delegata, ove istituita; il Ministro degli affari esteri e della cooperazione internazionale; il Ministro dell'interno; il Ministro della giustizia; il Ministro della difesa; il Ministro dell'economia e delle finanze; il Ministro dello sviluppo economico; il Ministro della transizione ecologica; il Ministro dell'università e della ricerca; il Ministro delegato per l'innovazione tecnologica e la transizione digitale; il Ministro delle infrastrutture e della mobilità sostenibili e, infine, come previsto dal comma 4, il direttore generale dell'ANC, che svolge le funzioni di segretario del Comitato.

Inoltre, ai sensi del comma 5, è previsto che il Presidente del Consiglio dei ministri possa chiamare a partecipare alle sedute del CIC, anche a seguito di loro richiesta, e senza diritto di voto, altri soggetti eventuali, quali gli altri Ministri oltre quelli componenti il Comitato, nonché le altre autorità civili e militari di cui, di volta in volta, si ritenga necessaria la presenza in relazione alle questioni da trattare.

2.2. L'Agenzia per la Cybersicurezza Nazionale: struttura, funzioni e autonomia

Gli artt. 5, 6 e 7 del decreto sono rispettivamente relativi, all'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), quale soggetto pubblico che svolge una funzione strumentale all'esercizio delle competenze che il decreto-legge assegna al Presidente del Consiglio dei ministri e all'Autorità delegata (art. 5, co. 2); all'organizzazione dell'Agenzia (art. 6); e alla disciplina delle sue funzioni e dei suoi compiti (art. 7). Negli artt. 11 e 12 è confluita la disciplina delle risorse finanziarie e autonomia contabile nonché la disciplina del personale dell'Agenzia.

Preme innanzitutto osservare che la scelta del modulo organizzativo ritenuto appropriato per l'istituzione di un soggetto pubblico deputato alla «tutela degli interessi nazionali nel campo della cybersicurezza»[27] è caduta su quello dell'agenzia amministrativa[28]. Riprendendo in parte una formulazione nota alla disciplina

[26] Il riferimento è a quelle condizioni di «rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi di cui all'articolo 1, comma 2, lettera b), e comunque nei casi di crisi cibernetica [...]» di cui all' art. 5, del decreto-legge del 21 settembre 2019, n. 105, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*", è stato convertito con modificazioni dalla l. 18 novembre 2019, n. 133.

[27] art. 5, co. 1, del d.l. n. 82/2021.

[28] In generale sulle agenzie amministrative v. G. ARENA, *L'esperienza delle agenzie nel sistema amministrativo svedese*, in *Riv. trim. dir. pubbl.*, 1974, pp. 69 ss.; ID., *Agenzia amministrativa*, in *Enc. giur. Treccani*, Roma, 1999, pp. 1 ss.; N BASSI, *Agenzie nazionali ed europee*, in *Enc. dir., Annali*, II, t. 2, Milano, 2009, pp. 41 ss.; H. CAROLI CASAVOLA, *L'amministrazione centrale*, in L. FIORENTINO (a cura di), *Le amministrazioni pubbliche tra conservazione e riforme*, Milano, 2008, pp. 1 ss.; L. CASINI, *Le agenzie amministrative*, in *Riv. trim. dir. pubbl.*, 2003, pp. 393 ss.; C. CORSI, *Agenzia e agenzie: una nuova categoria amministrativa?*, Torino, 2005; L. CASINI -E. CHITI, *L'organizzazione*, in G. NAPOLITANO (a cura di), *Diritto amministrativo comparato*, Milano, 2007, pp. 61 ss.; M. CLARICH – B.G. MATTARELLA, *L'Agenzia italiana del farmaco*, in G. FIORENTINI (a cura di), *I servizi sanitari in Italia*, Bologna, 2004, pp. 263 ss.; M. D'ALBERTI, *Lezioni di diritto amministrativo*, Torino, 2013, pp. 80 ss; C. TOVO, *Le agenzie decentrate dell'Unione Europea*, Napoli, 2016; L. FIORENTINO - A. STANCANELLI, *Le agenzie fiscali (articoli 57, 61-74)*, in S. PAJNO – L. TORCHIA (a cura di), *La riforma del governo*,

di dette figure, il comma 2 dell'art. 5 specifica infatti che l'ANC, «ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti di quanto previsto dal presente decreto». L'elevato *expertise* tecnico richiesto dalla materia, nonché l'esigenza di flessibilità e indipendenza dal potere politico nell'esercizio delle sue funzioni, si ritengono essere i motivi che hanno portato ad optare per questo modello organizzativo quale certamente più confacente alla garanzia di simili necessità[29]. Tuttavia, come precisato nel dossier del Servizio studi della Camera e del Senato che ha accompagnato la lettura del decreto, l'ACN si caratterizza per «una più marcata autonomia rispetto ad altre agenzie», tale da collocarla «al di fuori del modello di agenzia creato dal d.lgs. n. 300/1999»[30].

A tal proposito, al fine di cogliere i tratti caratterizzanti la nuova Istituzione, si è ritenuto utile declinare la trattazione nelle tre dimensioni - già adottate in dottrina per lo studio dei modelli di agenzia nel contesto internazionale[31] - rispettivamente relative: *a)* alla struttura organizzativa (con particolare riferimento agli organi di vertice); *b)* alle funzioni svolte e, *c)* all'autonomia.

a) La struttura organizzativa. Il decreto articola un'organizzazione di vertice analoga a quella delle agenzie amministrative di cui al decreto legislativo n. 300 del 1999, salvo l'assenza di un comitato di gestione. Gli art. 5, co. 3 e art. 6, co. 2 del decreto, dispongono infatti che l'Agenzia è costituita dal Direttore generale, dal Vice Direttore generale, e dal Collegio dei revisori dei conti.

L'art. 5 co. 3, pone il primo a capo dell'ANC, quale diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, nonché gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia di cui ha la rappresentanza legale. Circa la sua individuazione, sono previste elevate competenze, dato che il Direttore è nominato tra le categorie, tra cui può essere nominato il Segretario generale della Presidenza del Consiglio (art. 18, co. 2, L. n. 400 del 1988), ossia tra «i magistrati delle giurisdizioni superiori ordinaria ed amministrativa, gli avvocati dello Stato, i dirigenti generali dello Stato

Bologna, 2000, pp. 401 ss.; C. FRANCHINI, *L'organizzazione*, in S. CASSESE (a cura di), *Trattato di diritto amministrativo*, I, II ed., Milano, 2003, I, pp. 297 ss.; F. MERLONI, *Le agenzie nel sistema amministrativo italiano*, in *Dir. pubbl.*, n. 3, 1999, pp. 717 ss.; F. MERLONI, *Le agenzie a cinque anni dal d.lgs. n. 300: l'abbandono del modello generale?*, in G. VESPERINI (a cura di), *La riforma dell'organizzazione centrale*, Milano, 2005, pp. 21 ss.; G. NAPOLITANO, *L'Agenzia per l'acqua*, in *Giorn. dir. amm.*, 2011, pp. 1077 ss.; G. PETRONI, *Nuovi profili organizzativi dell'evoluzione del sistema amministrativo pubblico*, Padova, 1988; G. SCIULLO, *Alla ricerca del centro*, Bologna, 2000; G. VESPERINI, *Le agenzie (articoli 8-10)*, in S. PAJNO – L. TORCHIA (a cura di), *La riforma del governo*, Bologna, 2000, pp. 145 ss; G. SORICELLI, *Le agenzie amministrative nel quadro dell'organizzazione dei pubblici poteri*, Napoli, 2002.

[29] M.S. GIANNINI, *In principio sono le funzioni*, in *Amministrazione civile*, II, 3, 1959, pp. 11 ss.

[30] Cfr, A.C. 3161, Dossier su "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*", 23 luglio 2021, pp. 19 ss. (Il documento è disponibile sul sito della Camera dei deputati)

[31] Cfr. F. TOTH, *op. cit.*, p. 140.

ed equiparati, i professori universitari di ruolo ovvero tra estranei alla pubblica amministrazione», purché in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione[32]. Requisiti questi che la lettera del disposto non richiede espressamente anche per l'individuazione del Vice Direttore generale, sebbene si ritenga che questi possano certamente essere un parametro di valutazione anche per tale figura[33]. In entrambi i casi, il decreto-legge, prevede che i ruoli di Direttore generale e Vice Direttore generale abbiano una durata massima di quattro anni, salvo rinnovo con successivi provvedimenti per una durata complessiva massima di ulteriori quattro anni.

Per quanto riguarda il Collegio dei revisori dei conti, la sua composizione e le sue funzioni sono state individuate con il successivo d.P.C.M. del 9 dicembre 2021 n. 223, con cui è stato stabilito che il Collegio sia composto da un presidente individuato tra i magistrati della Corte dei conti, in servizio o in quiescenza; da un componente effettivo, designato dal Ministero dell'economia e delle finanze; e da un ulteriore componente effettivo e un componente supplente, scelti entrambi tra soggetti, in servizio o in quiescenza, appartenenti ai ruoli della magistratura amministrativa, contabile o dell'Avvocatura dello Stato, ovvero tra professori universitari ordinari di contabilità pubblica o discipline similari, ovvero tra alti dirigenti dello Stato[34].

Il d.P.C.M. in questione ha inoltre provveduto a dettare la disciplina dell'organizzazione interna dell'Agenzia, articolando una macrostruttura ripartita in Uffici di livello dirigenziale generale, ossia i "Servizi generali", e Uffici di livello dirigenziale non generale, le "Divisioni"[35].

Nello specifico, i primi «sono posti alle dipendenze del direttore generale dell'Agenzia e operano sulla base degli indirizzi dallo stesso forniti» negli ambiti direttamente correlati alle funzioni e alle politiche generali dell'ACN, mentre i secondi, operano all'interno dei Servizi e sono attivi nella «gestione di un insieme omogeneo di tematiche e macro-processi».

b) Le funzioni. L'art. 7 del decreto detta un'ampia articolazione di compiti attribuiti all'ACN. Tuttavia, prima di passare alla loro trattazione, si ritiene utile precisare preliminarmente che l'Agenzia è investita della tutela di un particolare aspetto della (cyber)sicurezza che può essere indicato, in considerazione della distinzione in uso negli ordinamenti anglosassoni tra *security* e *safety*, con il termine "*cyber-safety*", ossia l'ACN è destinataria di funzioni volte ad assicurare, nel senso più ampio del concetto di sicurezza,

[32] Conformemente al dettato dell'art. 2, co.1, lett. c) del decreto in oggetto, il 5 agosto 2021, il Presidente del Consiglio dei ministri, previa deliberazione del Consiglio dei ministri, e comunicazione al Presidente del COPASIR e alle Commissioni parlamentari competenti, ha nominato il Prof. Roberto Baldoni a Direttore generale dell'ACN.

[33] Il 6 ottobre 2021, il Presidente del Consiglio dei ministri ha nominato la Dott.ssa Nunzia Ciardi Vice Direttore generale dell'Agenzia.

[34] In particolare, l'art. 8, co. 5 del d.P.C.M. 9 dicembre 2021, n. 223, prevede che il Collegio: «a) effettua il riscontro degli atti della gestione finanziaria e formula le proprie osservazioni; b) svolge, almeno una volta ogni tre mesi, verifiche di cassa e di bilancio; c) esprime, in apposita relazione, parere sul progetto di bilancio preventivo, nonché sul rendiconto annuale; d) esercita ogni altra funzione ad esso attribuita dalla normativa vigente».

[35] Cfr. art. 6, co. 1, del decreto-legge 82/2021.

l'incolumità della collettività[36]. Ciò può essere dedotto dal contenuto della lett. n), ove è previsto che l'Agenzia «sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, [...]», grazie all'azione del CSIRT Italiano[37], organo trasferito presso l'ACN ai sensi dell'art. 7, co. 3 del decreto, e collocato nell'Ufficio dirigenziale generale del Servizio Operazioni in virtù del d.P.C.M. n. 223/2021[38].

Si desume pertanto che le competenze operative dell'Agenzia siano espressamente limitate ad attività che non interessano la sicurezza in senso stretto (*security*), quali le attività di *cyber investigation*, di competenza delle Forze di polizia; di *cyber-intelligence*, di competenza degli Organismi di informazione per la sicurezza; nonché di *cyber-defense*, intesa come difesa e sicurezza militare dello Stato, riconducibile all'area di competenza del Ministero della difesa[39], sebbene l'ACN, e il NC come si vedrà più avanti, collaborino attivamente con questi soggetti.

Entrando nel merito delle attribuzioni, si precisa che il citato d.P.C.M. n. 223/2021, in correlazione con le funzioni e le politiche dell'Agenzia, ha articolato l'organizzazione degli Uffici di livello dirigenziale generale secondo sette "Servizi", rispettivamente: Gabinetto; Autorità e sanzioni; Certificazione e vigilanza; Operazioni; Programmi industriali, tecnologici, di ricerca e formazione; Risorse umane e

[36] Sebbene la distinzione tra i concetti di "*security*" e "*safety*", ossia tra l'insieme delle azioni e degli strumenti in risposta ad una minaccia in atto, derivante da azione dolosa, organizzata cioè proprio allo scopo di arrecare danni (*security*), e l'insieme di misure e strumenti atti a prevenire o ridurre gli eventi accidentali che potrebbero causare ferite a persone o danni a cose (*safety*), sia propria degli ordinamenti anglosassoni, si ritiene opportuno ricorrere a questa distinzione al fine di meglio comprendere e agevolare l'analisi delle competenze attribuite all'Agenzia. Sul punto v. J. WALDRON, *Safety and Security*, in *Nebraska Law Review*, v. 85, 2006; M. DURANTE, *Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks*, in D. BERKICH, M. V. D'ALFONSO (a cura di), *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence*, Springer Nature, 2019, pp. 371 ss.

[37] Acronimo di *Computer Security Incident Response Team*, il CSIRT è un gruppo di intervento, normativamente inquadrato nella cornice costituita dagli artt. 9, 10 e 12 della direttiva (UE) 2016/1148 (c.d. direttiva NIS), gli artt. 8, 9 e 11 del decreto legislativo n. 65 del 2018, che ha recepito la citata direttiva nell'ordinamento italiano, nonché dal d.P.C.M. 8 agosto 2019 con il quale è stato istituito il CSIRT Italiano presso il Dipartimento delle Informazioni per la Sicurezza (DIS), e ora trasferito presso l'ACN in forza dell'art. 7, co. 3, del decreto-legge n. 82 del 2021. Il Gruppo è incaricato di monitorare gli incidenti a livello nazionale; emettere preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; intervenire in caso di incidente; analizzare dinamicamente i rischi e gli incidenti; svolgere attività di sensibilizzazione situazionale; prendere parte alla c.d. rete dei CSIRT che interloquisce con l'Agenzia dell'Unione europea per cybersicurezza (ENISA). Tale sigla viene spesso utilizzata in sostituzione di un altro acronimo, quello di CERT, ossia *Computer Emergency Response Team*, il quale svolge le medesime funzioni del CSIRT. La distinzione tra i due è infatti dovuta ad una questione di mero diritto dei marchi, in quanto il CERT nacque su iniziativa dell'agenzia statunitense DARPA (*Defence Advanced Research Projects Agency*), la quale istituì tale Gruppo presso la Carneige Mellon University di Pittsburgh in Pennsylvania che ne detiene ancora oggi la proprietà del marchio. Pertanto, la distinzione tra i due acronimi è che l'utilizzo della denominazione CSIRT è svicolata da obblighi derivanti dall'uso di marchi, e non richiede pertanto l'autorizzazione della Mellon University per il suo utilizzo. Più in generale, sull'evoluzione dei gruppi di gestione degli incidenti di sicurezza informatica v. A. CONTALDO, F. PELUSO, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa, 2018, pp. 70 ss

[38] Cfr. art. 12, co. 1, lett. s) del d.P.C.M. n 223/2021. s

[39] Tuttavia, l'art. 7, co. 1, lett. a) prevede che «per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera l), della legge n. 124 del 2007, sia le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge n. 124 del 2007».

strumentali; Strategie e cooperazione[40]. Sebbene tale suddivisione possa costituire un utile strumento per la disamina delle diverse competenze affidate all'ACN, si ritiene tuttavia che l'Agenzia, nell'esercizio complessivo delle sue funzioni, sia diretta alla realizzazione di quattro obiettivi principali, che interessano: *(i) l'esercizio di funzioni derivanti dalla qualifica di Autorità nazionale per la cybersicurezza*; *(ii)* il *coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale*; *(iii)* la *promozione 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*; *(iv)* il *conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore*[41].

Considerato che i numerosi compiti definiti all'art. 7 possono essere più affini alla realizzazione di un obiettivo piuttosto che di un altro, nell'analisi che segue si è ritenuto utile trattare tali attribuzioni nell'ambito dei quattro obiettivi appena citati, al fine di individuare una loro possibile categorizzazione e agevolarne la disamina.

(i) Iniziando con il *primo*, l'Agenzia è innanzitutto «Autorità nazionale per la cybersicurezza», qualifica che permette di comprendere e interpretare alcune attribuzioni[42], tra cui vi rientrano la predisposizione della strategia nazionale di cybersicurezza[43], nonché le assunzioni di compiti prima attribuiti ad altri soggetti,

[40] Cfr. art. 12 del d.P.C.M. n. 223/2021.

[41] Cfr. art. 7, co. 1, lett. a) del d.l. n. 82/2021.

[42] Si fa rispettivamente riferimento alle attribuzioni di cui all'art. 7, co. 1, lett. b), d), f), h), i), l), n), o), p), u), v), v-*bis*) del decreto-legge n. 82 del 2021.

[43] Si tratta di un documento la cui stesura è contemplata all'art. 7 della direttiva NIS, rubricato "*Strategia nazionale in materia di sicurezza della rete e dei sistemi informativi*". Come precisato nell'Allegato 1 della Comunicazione della Commissione europea, "*Sfruttare al meglio le reti e i sistemi informativi – verso l'efficace attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*", COM (2017)476 final del 4 ottobre 2017, tale strategia «è equiparabile alla "strategia nazionale di cybersicurezza" (NCSS)» (p. 5) (documento consultabile sul sito della Commissione europea). L'art. 6. co.1, del decreto legislativo 65/2018, con il quale l'Italia ha recepito la direttiva NIS, fa infatti riferimento alla NCSS, prevedendo al comma 2 che «nell'ambito della strategia nazionale di cybersicurezza, sono in particolare indicati, per la sicurezza di reti e sistemi informativi rientranti nell'ambito di applicazione del presente decreto: a) gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi informativi; b) il quadro di governance per conseguire gli obiettivi e le priorità, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; c) le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato; d) i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi; e) i piani di ricerca e sviluppo; f) un piano di valutazione dei rischi; g) l'elenco dei vari attori coinvolti nell'attuazione». Il co. 4 del decreto legislativo 65/2018, novellato a seguito dell'entrata in vigore del decreto-legge n. 82/2021, prevede inoltre che «l'Agenzia per la cybersicurezza trasmette la strategia nazionale in materia di cybersicurezza alla Commissione europea entro tre mesi dalla sua adozione. Può essere esclusa la trasmissione di elementi della strategia riguardanti la sicurezza nazionale».

[43] Cfr. art. 3 della l. 3 agosto 2007, n. 124, il quale prevede che «Il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare le funzioni che non sono ad esso attribuite in via esclusiva soltanto ad un Ministro senza portafoglio o ad un Sottosegretario di Stato, di seguito denominati "Autorità delegata". 2. L'Autorità delegata non può esercitare funzioni di governo ulteriori rispetto a quelle ad essa delegate dal Presidente del Consiglio dei ministri a norma della presente legge. 3. Il Presidente del Consiglio dei ministri è costantemente informato dall'Autorità delegata sulle modalità di esercizio delle funzioni delegate e, fermo restando il potere di direttiva, può in qualsiasi momento avocare l'esercizio di tutte o di alcune di esse. 4. In deroga a quanto previsto dal comma 1 dell'articolo 9 della legge 23 agosto 1988, n. 400, e successive modificazioni, non è richiesto il parere del Consiglio dei ministri per il conferimento delle deleghe di cui al presente articolo al Ministro senza portafoglio».

quali, il Ministero dello sviluppo economico (MISE), la Presidenza del Consiglio dei ministri, il Dipartimento delle informazioni e della sicurezza (DIS) e l'Agenzia per l'Italia digitale (AgID).

In particolare, per quanto riguarda il MISE, la lett. f) prevede che l'ACN «assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico» ivi comprese quelle relative al Perimetro di Sicurezza Nazionale Cibernetica (n. 1), alla sicurezza ed integrità delle informazioni elettroniche (n. 2)[44], alla sicurezza delle reti e dei sistemi informativi di cui alla disciplina italiana che ha recepito la direttiva NIS (n. 3). Si precisa che, in virtù delle attribuzioni di cui al n. 1, l'Agenzia può condurre attività di ispezione, verifica e accertamento delle violazioni da parte dei soggetti privati afferenti al PSNC, potendo anche impartire, se necessario, specifiche prescrizioni, nonché irrogare sanzioni amministrative previste dal decreto istitutivo il PSNC. Preme inoltre osservare che, in virtù di tali acquisizioni, l'Agenzia è depositaria delle funzioni attribuite al Centro di Valutazione e Certificazione Nazionale (CVCN) - ora trasferito presso la stessa ai sensi dell'art. 7, co. 4, del decreto – quale organo competente nella valutazione tecnica di prodotti e sistemi ICT impiegati da soggetti titolari di funzioni critiche o strategiche.

Il dettato della lett. h) integra invece la sfera di competenze appena analizzate, in quanto trasferisce all'ACN i compiti prima attribuiti alla Presidenza del Consiglio in materia di PSNC - escluse le attribuzioni contemplate all'art. 3 del d.P.C.M. n. 131 del 2020, relative all'individuazione dei soggetti rientranti nel perimetro, per il settore spazio, aerospazio e tecnologie critiche che restano di competenza di quest'ultimo[45] - permettendo all'Agenzia di condurre attività di ispezione e verifica anche su soggetti pubblici afferenti al Perimetro, conferendole così un generale potere di ispezione, verifica e accertamento delle violazioni su tutti i soggetti, sia pubblici che privati, afferenti il PSNC.

Ai sensi della lett. i), l'Agenzia acquisisce tutte le funzioni che il decreto-legge istitutivo il PSNC, e i relativi provvedimenti attuativi, attribuivano al DIS. In virtù di ciò, l'ACN è quindi destinataria delle notifiche degli incidenti di sicurezza da parte dei soggetti coinvolti in attacchi informatici[46], ed inoltre supporta il Presidente del Consiglio nel coordinamento e attuazione delle disposizioni che disciplinano il PSNC[47].

[44] Il riferimento è agli artt. 16-bis e 16-ter del decreto legislativo 1 agosto 2003, n. 259, attributivi di funzioni al Ministero per lo sviluppo economico circa l'individuazione delle misure di natura tecnica e organizzativa per assicurare la sicurezza delle reti e dei servizi; il controllo previsto sulle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico.

[45] Si intendono le tecnologie di cui all'art. 4, par. 1, lett. b), del Reg. (UE) 2019/452, ossia quelle tecnologie, tra cui figurano «l'intelligenza artificiale, la robotica, i semiconduttori, la cybersicurezza, le tecnologie aerospaziali, di difesa, di stoccaggio dell'energia, quantistica e nucleare, nonché le nanotecnologie e le biotecnologie».

[46] Ai sensi dell'art. 1, lett. h) del d.P.C.M. 14 aprile 2021, n. 81, con la nozione di "incidente" di cybersicurezza, si intende «ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici».

[47] Cfr. art. 1, comma 19-bis, del decreto-legge 105 del 2019.

Su quest'ultimo punto si ritiene che tale attività potrebbe comportare dubbi interpretativi circa la titolarità formale dell'atto di assunzione delle determinazioni in caso di c.d. "crisi cibernetica", di cui all'art. 5 del decreto istitutivo il PSNC, consistente nella «disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati» in caso di «rischio grave e imminente per la sicurezza nazionale»[48]. Tuttavia, alla luce del dettato di cui alla lett. l), ove è stabilito che l'ACN «provvede, 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 dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro»[49], è possibile concludere che la titolarità di tali determinazioni continui ad essere affidata – come ragionevole - al solo Presidente del Consiglio dei ministri.

Infine, per quanto riguarda i compiti prima attribuiti all'AgID, la nuova normativa trasferisce all'Agenzia la responsabilità della sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni, nonché l'adozione delle linee guida contenenti regole tecniche di cybersicurezza, conformemente a quanto disposto negli artt. 51 e 71 del d.lgs. 7 marzo 2005, n. 82 (c.d. Codice per l'Amministrazione Digitale – CAD).

Al pari delle altre agenzie amministrative di carattere speciale, l'ACN è inoltre chiamata a svolgere funzioni di carattere tecnico-operativo[50], affiancando ambiti di attività che richiedono elevate competenze tecnico-scientifiche, ad attribuzioni di alta consulenza e collaborazione con soggetti istituzionali pubblici

[48] Si tratta della disciplina relativa alle «determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica», ove sono disciplinate le attribuzioni emergenziali in capo alla Presidenza del Consiglio dei ministri in presenza «di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici». Nello specifico, il disposto prevede che il Presidente del Consiglio, su deliberazione del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), possa disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati, e che ne fornisca informazioni entro trenta giorni al COPASIR. Preme precisare che tale intervento deve essere disposto «per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità». Le cautele, riconducibili alla limitazione del tempo di disattivazione e al criterio di proporzionalità, costituiscono dei parametri di garanzia dei servizi e delle funzioni interessate dalla disciplina del PSNC. Difatti, uno *shutdown*, anche solo parziale, di tali attività essenziali potrebbe comportare problemi sotto i profili del ripristino e della continuità delle stesse. Ragione per cui si ritiene che tale misura deve essere intesa come una *extrema ratio*.

[49] Cfr. art. 7, co. 1, lett. l) del d.l. n. 82/2021.

[50] Per altre agenzie amministrative che svolgono funzioni tecnico-operative, v. ad esempio l'Agenzia spaziale italiana (l. 30.5.1988, n. 186, e successive modificazioni), l'Agenzia per la rappresentanza negoziale nelle pubbliche amministrazioni - Aran (art. 50, d.lgs. 3.2.1993, n. 29, ora art. 46, d.lgs. 30.3.2001, n. 165), l'Agenzia nazionale per la protezione dell'ambiente - Anpa (istituita nel 1993 e soppressa nel 1999). Sulla discontinuità del carattere tecnico-operativo delle agenzie amministrative disciplinate dal decreto legislativo n. 300 del 1999 rispetto a quelle regolate dal sistema previgente, v. F. MERLONI, *Il nuovo modello di agenzia nella riforma dei ministeri*, in *Dir. pubbl.*, n. 3, 1999, pp. 720 ss, ove l'A., in riferimento allo scritto di G. ARENA, *Agenzia amministrativa*, cit., rileva come le agenzie pre-d.lgs. n. 300 del 1999, si caratterizzassero tutte per lo svolgimento di attività strettamente tecniche (e non anche operative).

e privati, anche a livello internazionale[51]. Tali profili, ossia, quello tecnico e quello operativo, trovano espressione nelle diverse attività di promozione della ricerca e formazione nell'ambito della cybersicurezza, i cui risultati (ad esempio, scoperte nel campo informatico, nuovi standard ecc.), andranno a costituire, come è ragionevole credere, il tratto caratterizzante l'attività di consulenza e supporto tecnico prestato dall'ACN[52]. In particolare, si osserva che, l'azione dell'Agenzia in tale contesto, con il supporto dell'organo interno del Comitato tecnico-scientifico[53], consiste nel farsi promotrice, sviluppatrice e finanziatrice di attività formative e di ricerca nel settore, attraverso il coinvolgimento di una moltitudine di soggetti impegnati in tali attività: nello specifico, università, enti di ricerca nonché il sistema produttivo nazionale, attraverso il ricorso ad una serie di strumenti. Relativamente ai primi due soggetti, il sistema universitario e quello della ricerca, l'Agenzia favorisce l'attivazione di percorsi formativi «anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati», con la possibilità di utilizzare per tali fini «[le] strutture formative e [le] capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno»[54].

Per quanto riguarda invece il coinvolgimento dei soggetti operanti nel sistema produttivo nazionale, la lett. z) prevede la costituzione di partenariati pubblico-privati, o la costituzione e partecipazione a consorzi, fondazioni o società con soggetti pubblici e privati italiani, previa autorizzazione del Presidente del Consiglio dei ministri, al fine di stimolare la produzione e l'innovazione in questo settore[55].

Ulteriore soggetto coinvolto in tali attività di ricerca e formazione è il Ministero della difesa, il quale, a seguito di una modifica introdotta in sede di conversione, è stato designato quale soggetto pubblico

[51] In particolare, su quest'ultimo punto si faccia riferimento alle attribuzioni di cui all'art. 7, co. 1, lett. o) ove è previsto che l'ACN «partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese».

[52] Cfr. lett. r) del decreto, ove è previsto che «l'Agenzia può promuovere, sviluppare e finanziar specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore», oltreché «promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo».

[53] Il Comitato tecnico-scientifico, presieduto dal Direttore generale, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, ai sensi dell'art. 11, del d.P.C.M. n. 223/2021 è «volto a promuovere la collaborazione con il sistema dell'università e della ricerca e con il sistema produttivo nazionale, nonché a supportare le iniziative pubblico-private in materia di cybersicurezza».

[54] Cfr. lett. v) del decreto. Si precisa che le modalità e i termini di tale avvalimento saranno definiti con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati, e pertanto, nelle more della promulgazione del decreto, sembra utile chiedersi quale grado di autonomia sarà garantito alle ricerche svolte all'interno di tali amministrazioni. Sul punto v. F. MERLONI, *Autonomie e libertà nel sistema della ricerca scientifica*, Milano, 1990.

[55] Sul partenariato pubblico-privato in generale v. D. SICLARI, *Il project financing nel codice dei contratti pubblici. Problemi e prospettive*, Torino, 2019. Sul partenariato pubblico-privato nell'ambito della cybersicurezza v. E. CAMPAGNANO, *Le Nuove Forme del Partenariato Pubblico-Privato. Servizi pubblici e infrastrutture*, Padova, 2020.

competente per gli aspetti inerenti alla ricerca in campo di cybersicurezza militare e con i quali l'Agenzia dovrà addivenire ad un «necessario raccordo»[56].

Sempre all'interno di questo ambito, può essere collocato anche la promozione e lo sviluppo di una cultura della cybersicurezza volta a fornire maggiore consapevolezza (*awareness*) della popolazione in materia (sul punto si rinvia al par. 3).

Particolarmente rilevante appare inoltre l'attribuzione di cui alla lett. p), secondo cui l'Agenzia è chiamata a prestare il suo supporto in ambito legislativo e regolamentare, fornendo pareri non vincolanti sulle iniziative normative in materia di cybersicurezza, con lo scopo di curare e promuovere «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». È ragionevole ritenere che tale attribuzione, connessa con la precedente, lasci intuire la realizzazione di future collaborazioni tra studiosi ed esperti sia di sicurezza informatica, sia del diritto, e delle altre scienze sociali, al fine di fornire un sostanziale supporto nella creazione di una *governance* di cybersicurezza frutto delle esperienze degli esperti di settore.

(ii) Alle attività di «*coordinamento dei soggetti pubblici coinvolti nella sicurezza cibernetica nazionale*» possono essere ricondotte più in generale le collaborazioni istituzionali con altri organi dello Stato e con le altre amministrazioni, tra cui ad esempio, il Garante per la protezione dei dati personali (vedi di seguito) o altre Autorità indipendenti, le Forze armate e di polizia e gli altri enti pubblici.

In attesa di accordi di collaborazione in tal senso, dalla lettera del decreto legge è tuttavia possibile individuare delle sicure collaborazioni, di cui nello specifico: le attività di supporto al funzionamento del Nucleo per la Cybersicurezza[57]; la partecipazione al c.d. Tavolo Perimetro, quale Organo interministeriale istituito a supporto del CISR tecnico ai sensi dell'articolo 6, comma 1, del d.P.C.M. 30 luglio 2020, n. 131, per l'attuazione del PSNC, nonché al Comitato tecnico di raccordo, istituito presso la Presidenza del Consiglio dei ministri per l'adempimento degli obblighi derivanti dal d.lgs. 18 maggio 2018, n. 65 recettivo della direttiva NIS; la partecipazione al gruppo di coordinamento istituito dalle disposizioni attuative del decreto-legge n. 21 del 2012[58]; il coordinamento, in raccordo con il Ministero degli affari esteri e della

[56] Cfr. lett. r) del decreto. Alla luce delle considerazioni sin qui svolte in merito all'attività di promozione e sviluppo della formazione e della ricerca nell'ambito della cybersicurezza da parte dell'Agenzia, sembra utile chiedersi quale grado di autonomia sarà riservato alle ricerche considerata la diversa natura dei soggetti coinvolti. Sul punto si consiglia F. MERLONI, *op. cit.*, 1990; A.M. SANDULLI, *L'autonomia delle università statali*, in A.A.V.V., *Scritti in memoria di Luigi Cosattini*, Trieste, 1948.

[57] Cfr. lett. c) del decreto.

[58] Cfr. art. 7, co. 1, lett. g) del decreto-legge n. 82 del 2021. Il riferimento è al d.P.R. n. 35 del 2014, adottato a norma dell'articolo 1, comma 8, del decreto-legge n. 21 del 2012, il quale prevede l'istituzione da parte del Presidente del Consiglio di un gruppo di coordinamento, presieduto da apposito ufficio della medesima Presidenza del Consiglio (o da altro componente da lui indicato) e dai responsabili dei corrispettivi uffici Ministri dell'economia e delle finanze, della difesa, dell'interno, dello sviluppo economico e degli affari esteri (salva integrazioni con altri componenti). Sulla

cooperazione internazionale, delle politiche in materia di cybersicurezza[59]; ed infine, il già ricordato coinvolgimento delle università e della ricerca, al fine di sviluppare competenze e capacità industriali, tecnologiche e scientifiche nel campo della cybersicurezza.

(iii) Si ritiene invece possano essere riferiti all'*obiettivo* della *promozione 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»*, i compiti relativi alla valorizzazione della misura di sicurezza della crittografia[60]; alla qualificazione dei servizi *cloud* per la pubblica amministrazione[61]; alla stipula di accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale[62]; la promozione della partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della

disciplina dei golden powers v. F. FORTUNA, *I poteri speciali esercitabili da parte dell'esecutivo*, in R. MICCÙ (a cura di), *Un nuovo diritto delle società pubbliche? Processi di razionalizzazione tra spinte all'efficienza e ambiti di specialità*, Napoli, 2019., pp.343 ss; G. DELLA CANANEA, L. FIORENTINO, *I "poteri speciali" del Governo nei settori strategici*, Napoli, 2020.

[59] Cfr. art. 7, co. 1, lett. q) del decreto-legge n. 82 del 2021. In particolare, il disposto precisa che «nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni ed enti, nonché segue nelle competenti sedi istituzionali le tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri»

[60] Cfr. art. 7, co. 1, lett. m-*bis*) del decreto-legge n. 82 del 2021, ove è precisato che l'ACN può farsi promotrice di tale iniziativa «anche attraverso un'apposita sezione dedicata nell'ambito della strategia di cui alla lettera b). In particolare, l'Agenzia attiva ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali». Brevemente, si precisa che la crittografia (informatica) è una tecnica che permette di preservare la sicurezza delle informazioni, ossia la loro riservatezza, integrità e disponibilità (c.d. triade del RID) codificando l'informazione attraverso una c.d. chiave di cifratura. Essa rappresenta infatti una delle misure di sicurezza che il titolare del trattamento dei dati personali è tenuto ad implementare ai sensi dell'art. 25 del Reg. (Ue) 679 del 2016 (GDPR).

[61] Cfr. art. 7, co. 1, lett. m-*ter*) del decreto-legge n. 82 del 2021. In particolare, il disposto prevede che l'Agenzia è tenuta al rispetto del regolamento di cui all'articolo 33-*septies*, co. 4, del decreto-legge n. 179 del 2012, sul "*Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese*" ove è previsto che «L'Agenzia per la cybersicurezza nazionale, con proprio regolamento, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri, nel rispetto della disciplina introdotta dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 [istitutivo del PSNC], stabilisce i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione, ivi incluse le infrastrutture di cui ai commi 1 e 4-*ter*. Definisce, inoltre, le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi cloud per la pubblica amministrazione. Con lo stesso regolamento sono individuati i termini e le modalità con cui le amministrazioni devono effettuare le migrazioni di cui ai commi 1 e 1-*bis*». A tal proposito, è d'uopo osservare che la realizzazione del c.d. *cloud* pubblico, costituisce uno degli obiettivi funzionali alla prima componente della missione 1 del Piano Nazionale Ripresa Resilienza (PNRR) sulla "digitalizzazione, innovazione e sicurezza nella PA". Pertanto, ai sensi del disposto in commento, è facile intuire che l'ACN svolgerà una funzione di supporto al fine di garantire la protezione e la sicurezza dell'architettura *cloud* nazionale delineata nel Piano.

[62] Cfr. art. 7, co. 1, lett. s) del decreto-legge n. 82 del 2021.

cybersicurezza[63]; la costituzione e partecipazione a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri[64]; ed infine, l'assunzione di tutte le funzioni già attribuite all'Agenzia per l'Italia digitale (AgID) in materia di cybersicurezza[65].

(iv) Infine, l'*obiettivo* relativo al *«conseguimento dell'autonomia nazionale ed europea su prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore della sicurezza cibernetica»* rappresenta un tema di estrema attualità, funzionale all'affermazione della c.d. sovranità digitale[66], concetto che ha assunto una varietà di significati a livello internazionale[67].

Nel "*consultation paper*" elaborato dall'ENISA nel 2019 avente ad oggetto il tema delle politiche industriali dei prodotti ICT nell'Unione, l'Agenzia europea ha ricondotto nella nozione di "sovranità digitale", tre diverse categorie concettuali, quali: la sovranità sui dati personali dei cittadini europei; la sovranità digitale dell'industria europea guidata dai dati; la sovranità digitale dell'Unione e degli Stati membri che la compongono[68]. L'obiettivo *(iv)* interessa certamente la seconda categoria, quella attinente all'aspetto industriale, il cui fine è quello di garantire una posizione di autonomia strategica dell'Unione europea,

---

[63] Cfr. art. 7, co. 1, lett. t) del decreto-legge n. 82 del 2021.

[64] Cfr. art. 7, co. 1, lett. z) del decreto-legge n. 82 del 2021.

[65] Cfr. art. 7, co. 1, lett. m) del decreto-legge n. 82 del 2021. Nello specifico il dettato normativo fa riferimento agli artt. 51 e 71 del decreto legislativo 7 marzo 2005, n. 82, rubricato "*Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni*", il quale attribuiva all'AgID l'attuazione per quanto di competenza e in raccordo con le altre autorità competenti in materia del Quadro strategico nazionale per la sicurezza dello spazio cibernetico (QSN) e del Piano nazionale per la sicurezza cibernetica e la sicurezza informatica (PN) – cfr. art. 51 - nonché l'adozione delle linee guida contenenti le regole tecniche e di indirizzo per l'attuazione – cfr. art. 71. Il risposto in commento prevede inoltre che l'Agenzi assume anche i compiti, già attribuiti all'AgID, di cui all'art. 33-*septies*, co. 4 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, rubricato "*Consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese*" ove è previsto che la determinazione, con proprio regolamento, dei livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione, ivi inclusi i Centri per l'elaborazione delle informazioni (CED), nonché delle caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi *cloud* per la pubblica amministrazione, e ancora i termini e le modalità con cui le amministrazioni debbano effettuare le migrazioni previste da quell'articolo 33-*septies*.

[66] *Ex multis*, V. ZENO -ZENCHOVIC, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4/5, vol. 31, 2017, pp. 683 – 696; E. MAESTRI, *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Ars interpretandi, Rivista di ermeneutica giuridica*, n. 1, 2017, pp. 15-28; G. TIBERI, *Il caso Schrems II: sovranità digitale europea o colonialismo giudiziario?*, in *Quaderni costituzionali, Rivista italiana di diritto costituzionale*, n. 1, 2021, pp. 231-234; V. PAGNANELLI, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Rivista italiana di informatica e diritto*, fasc. 1, 2021; L. CALIFANO, *Come si governa la tecnologia digitale?*, in *Cultura Giuridica e Diritto Vivente*, v. 8, 2021; M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in *Gruppo di Pisa*, fasc. n. 2, 2021. Analogamente vedi il concetto di "sovranità tecnologica europea" a cui ha fatto riferimento nel recente discorso "sulla stato dell'Unione" la Presidente Ursula von der Leyen, il 15 settembre 2021 a Strasburgo (il documento è consultabile sul sito della Commissione europea).(spostare alla nota sotto?)

[67] Sul punto v. S. COUTURE - S. TOUPIN, *What does the notion of "sovereignty" mean when referring to the digital?,* in *New Media & Society*, 21(10), 2019, pp. 2305-2322.

[68] Cfr. ENISA, *Consultation paper – EU ICT industrial policy: Breaking the cycle of failure*, 2019, p. 10 (il documento è consultabile sul sito dell'ENISA).

ossia «la capacità dell'Europa di procurarsi prodotti e servizi che soddisfano i suoi bisogni e valori, senza indebite influenze dal mondo esterno» nell'acquisto e implementazione di prodotti e servizi ICT[69].

Il tema investe diverse questioni, prima fra tutte quella relativa alla catena di approvvigionamento di tali prodotti e servizi, la c.d. *supply chain*, ossia quell'insieme di processi che interessano la distribuzione di *hardware* e *software*, *storage* in *cloud* o locale, a cui deve essere garantito un certo livello di affidabilità in termini di sicurezza informatica[70]. L'altra questione interessa l'*indipendenza* dell'Unione europea dalla catena di approvvigionamento di prodotti e servizi ICT provenienti da Paesi extra-Ue, sebbene al momento l'Unione non disponga ancora di sufficienti capacità, né di mezzi tecnologici e industriali, per garantire autonomamente la sicurezza della propria economia e delle proprie infrastrutture critiche[71].

È alla luce di tali considerazioni che si ritiene debbano essere interpretate le funzioni di cui all'art. 7, co. 1, lett. e) e aa), ove l'ACN viene rispettivamente qualificata "Autorità Nazionale di Certificazione della Cybersicurezza", di cui all'art. 58 del Reg. (UE) 2019/881, e designata "Centro Nazionale di Coordinamento" di cui all'art. 6 del Reg. (UE) 2021/887.

Relativamente alla prima funzione, con il citato Reg. (UE) 2019/881, anche noto come "*Cybersecurity Act*", l'Unione ha istituito il "Quadro europeo di certificazione della cybersicurezza", ossia un sistema comune di normative tecniche[72], utili alla certificazione o valutazione dei prodotti, servizi e processi ICT, con il fine di aumentare la fiducia dei cittadini, delle organizzazioni e delle imprese nel mercato unico digitale[73].

---

[69] ENISA, *Cybersecurity research directions for the Eu's digital strategic autonomy*, 2019, p. 5 (il documento è consultabile sul sito dell'ENISA).

[70] In particolare, le vulnerabilità che affliggono i prodotti e servizi ICT nelle catene di approvvigionamento possono essere sfruttate dai criminali informatici per veicolare *supply chain attacks*, ossia azioni volte ad infettare componenti *software* o *hardware* a monte, ossia in fase di produzione, distribuzione o manutenzione e aggiornamento. In tal modo, compromesso il fornitore di tali prodotti e servizi, gli effetti dell'attacco potranno facilmente estendersi anche a valle, verso gli acquirenti e utilizzatori finali. Sul punto si consiglia la lettura del documento dell'ENISA, *Threat Landscape for Supply Chain Attacks*, 2021 (il documento è disponibile sul sito dell'ENISA).

[71] Cfr. considerando 12, del Reg. (UE) 2021/887, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

[72] In generale, sulle norme tecniche e le certificazioni *ex multis* v. A. IANNUZZI, *Il diritto capovolto. Regolazione e contenuto tecnico-scientifico e Costituzione*, Napoli, 2018; A. MOSCARINI, *Fonti dei privati e globalizzazione*, Roma, 2015; F. SALMONI, *Le norme tecniche*, Milano, 2001; F. ANCORA, *Normazione tecnica, certificazione di qualità e ordinamento giuridico*, Torino, 2000; N. GRECO, *Crisi del diritto, produzione normativa e democrazia degli interessi. Esemplarità della normazione tecnica ambientale*, Roma, 1999; P. ANDREINI – G. CAIA – G. ELIAS – F.A. ROVERSI MONACO (a cura di), *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, Bologna, 1995; W. CESARINI SFORZA, *Il diritto dei privati*, Milano, 1963.

[73] Cfr. considerando 7, 48, 69 e art. 46 del Reg. (UE) 2019/881, *relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Reg. (UE) n. 526/2013 («regolamento sulla cybersicurezza»)*. L'art. 2, n. 9 del citato Regolamento, definisce il sistema europeo di certificazione della cybersicurezza come «una serie completa, di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti TIC, servizi TIC e processi TIC», mentre al n. 11, trova definizione la nozione di certificato europeo di cybersicurezza, inteso come «un documento rilasciato dall'organismo pertinente che attesta che un determinato prodotto TIC, servizio TIC o processo TIC è stato oggetto di una valutazione di conformità con i requisiti di sicurezza specifici stabiliti da un sistema europeo di certificazione della cybersicurezza».

Si precisa che il ricorso a tale schema sia al momento volontario, dato che solo a partire dal 2024 la Commissione europea potrà ritenere di rendere obbligatorio uno specifico sistema di certificazione in tutta l'Unione[74], e che, tuttavia, in mancanza di un diritto dell'Unione armonizzato, il citato Regolamento prevede che «gli Stati membri possono adottare regolamentazioni tecniche nazionali in cui sia prevista una certificazione obbligatoria nel quadro di un sistema europeo di certificazione della cibersicurezza in virtù della direttiva (UE) 2015/1535»[75]. Pertanto, è ragionevole ritenere, che l'obiettivo relativo al conseguimento dell'autonomia nazionale su prodotti e processi informatici di rilevanza strategica perseguito dall'Agenzia, nelle more che il Quadro europeo di cybersicurezza acquisti piena cogenza, impone comunque la necessaria preparazione a tale nuovo sistema sul piano nazionale.

Simile interpretazione trova conferma nella previsione del d.P.C.M. n. 223/2021, ove è stabilito che l'ACN, per mezzo del Servizio Certificazione e vigilanza, «sovrintende ai processi di certificazione, qualificazione e valutazione»[76], ed in particolare assolve al ruolo di autorità nazionale di certificazione, supervisionando e facendo applicare le regole previste nei sistemi europei di certificazione della cybersicurezza[77].

In particolare, alla lett. e), del decreto legge in esame, è previsto che l'Agenzia è responsabile dell'accreditamento delle strutture specializzate del Ministero della difesa e del Ministero dell'interno, quali organismi di valutazione della conformità per i sistemi di rispettiva competenza, ai sensi dell'art. 60, par. 1, del Reg. (UE) 2019/881 (n. 1); e che la stessa possa delegare il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate, al rilascio del certificato europeo di cybersicurezza conformemente a quanto previsto dall'art. 56, par, 6, lett. b), del Reg. (UE) 2019/881 (n. 2).

La designazione dell'Agenzia quale "Centro Nazionale di Coordinamento", costituisce il primo passo verso la concreta realizzazione della c.d. autonomia strategica nazionale ed europea nell'ambito della cyberiscurezza. In virtù di tale prescrizione, l'ACN entra a far parte della *rete di centri nazionali di coordinamento,* il cui compito è quello di assistere il Centro di competenza europeo nell'assolvimento della sua missione e nel conseguimento dei suoi obiettivi, tra cui troviamo, il sostegno dell'industria della cybersicurezza, al fine di rafforzare l'eccellenza, la capacità e la competitività dell'Unione in tale settore[78]. Difatti, come rilevato nel documento dell'ENISA sull'autonomia strategica europea, la possibile violazione dei diritti fondamentali, dovuta all'implementazione da parte di Paesi extra-Ue di *hardware*,

[74] art. 56, co. 2 e 3, del Reg. (UE) 2019/881.
[75] Cfr. considerando 91 e art. 56 del Reg. (UE) 2019/881.
[76] art. 12, co. 2, lett. c) del d.P.C.M. n. 223/2021.
[77] Cfr. art. 12, co. 2, lett. c) n. 4 del d.P.C.M. n. 223/2021, ove viene fatto espresso rinvio all'art. 58 del Reg. (UE) 2019/881.
[78] Cfr. 5, par. 2, lett. b), ii, del Reg. (UE) 2021/887.

software e algoritmi non sviluppati in ossequio al rispetto di tali diritti, implicherebbe per l'Europa la necessaria produzione di tali beni in modo indipendente[79].

c) L'autonomia. Dopo aver esaminato la struttura e le funzioni, è ora possibile analizzare l'ultima dimensione, quella dell'autonomia. Come osservato da Alcuni, la "dispersione terminologica" sui vari concetti di autonomia, impedisce di addivenire ad una considerazione globale del fenomeno[80]; proprio per questo motivo, si è ritenuto utile concentrare la trattazione su due principali accezioni caratterizzanti l'autonomia dell'Agenzia, rispettivamente quella normativa e quella organizzativa.

Con la prima si intende la «capacità di emanare norme giuridiche equiparate a quelle dello Stato»[81], precisiamo tuttavia che al di fuori dei casi tassativamente previsti dall'ordinamento, tale capacità si esprime con l'emanazione di atti sub legislativi[82]. La precisazione è particolarmente utile nel caso dell'ACN, dato che, come già ricordato, ai sensi dell'art. 5 comma 2 del presente decreto-legge, questa «è dotata di autonomia regolamentare [...] nei limiti di quanto previsto dal presente decreto».

In particolare, il recente d.P.C.M. n. 223/2021, intervenendo sull'organizzazione e il funzionamento dell'Agenzia, ha contribuito alla definizione di tale aspetto, prevedendo che il Direttore generale «adotta ogni provvedimento, tra cui regolamenti e disciplinari, necessario all'attuazione delle funzioni dell'Agenzia, anche in attuazione della normativa vigente»[83].

Preme inoltre precisare che, sebbene non si tratti di un vero e proprio potere regolamentare, la citata decretazione dispone che anche alcuni Servizi, comunque rimessi agli indirizzi del Direttore generale, si esprimano con atti, di cui nello specifico: con pareri non vincolanti «su rilevanti iniziative legislative o regolamentari [...] al fine della definizione e del mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza», come nel caso del Gabinetto[84]; con linee guida contenenti regole tecniche di cybersicurezza della pubblica amministrazione, o la definizione di «misure di sicurezza e delle soglie di significatività degli incidenti riguardanti le reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico», oppure con la definizione «livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica

[79] Cfr, ENISA, *Cybersecurity research directions for the Eu's digital strategic autonomy*, 2021, p. 5. In particolare, in uno degli scenari proposti nel documento, in relazione a impedimenti relativi alla *supply chain* viene evidenziato che «i problemi della catena di approvvigionamento possono risultare in una mancanza di disponibilità di componenti elettronici richiesti dall'industria dell'UE. Senza tali componenti (ad esempio processori e chip), la fornitura di dispositivi elettronici personali e di elementi dell'infrastruttura digitale non può essere garantita, il che mette potenzialmente in pericolo l'autonomia strategica dell'Europa nelle industrie che dipendono la fornitura di dispositivi, come l'industria automobilistica».

[80] Cfr. F. MERLONI, *Autonomie e libertà nel sistema della ricerca scientifica*, cit., p. 101 ss.

[81] M.S. GIANNINI, *voce Autonomia b) Teoria gen.e dir. pubbl.*, in *Enciclopedia del diritto*, vol. IV, Milano, 1959, p. 358.

[82] F. MERLONI, *Autonomie e libertà nel sistema della ricerca scientifica*, cit., p. 113.

[83] art. 16 del d.P.C.M. n. 223/2021.

[84] art. 12, co. 2, lett. a) n. 4 del d.P.C.M. n. 223/2021.

amministrazione», come nel caso del Servizio autorità e sanzioni[85]. Nonché, infine, la competenza del Servizio strategie e cooperazione di definire «gli indirizzi strategici e gli strumenti di *policy* nazionali in materia di cybersicurezza»[86].

Passando al successivo profilo, analogamente, anche l'autonomia organizzativa trova espressione per mezzo dell'autonomia regolamentare. Diversi disposti del già richiamato d.P.C.M. conferiscono infatti al Direttore generale la possibilità di definire con provvedimenti generali l'organizzazione interna dell'ACN, ad esempio adottando la «pianificazione strategica dell'Agenzia, individuando gli obiettivi da conseguire, assegnandoli ai Capi dei Servizi», o adottando i «provvedimenti necessari per l'impiego delle risorse strumentali», nonché disponendo «le nomine, le promozioni, le assegnazioni, i trasferimenti e gli incarichi del personale»[87], oppure, su deliberazione del Comitato di Vertice, disponendo le nomine del presidente e dei componenti del Collegio dei revisori dei conti[88] e, sentito il Vice direttore, disponendo la nomina dell'Organismo indipendente di valutazione (OIV).

Infine, per quanto riguarda l'organizzazione sotto il profilo finanziario, tra i diversi aspetti relativi alla regolazione della contabilità dell'ACN, si evidenzia che l'art. 11, comma 2 del decreto legge, riconosce all'Agenzia la possibilità di trarre utili dalle attività svolte, tra cui, dai servizi prestati a soggetti pubblici o privati, proventi derivanti dallo sfruttamento della proprietà industriale, dei prodotti dell'ingegno e delle invenzioni, nonché contributi dell'Unione europea o di organismi internazionali, anche a seguito della partecipazione a specifici bandi, progetti e programmi di collaborazione, e i proventi delle sanzioni irrogate dall'Agenzia[89].

Si ritiene ora doveroso fare riferimento anche agli aspetti relativi ai rapporti tra l'Agenzia e le altre amministrazioni, in particolar modo rispetto a quelle di vigilanza.

A livello europeo, l'Agenzia è, a tutti gli effetti, parte integrante dell'ordinamento amministrativo europeo di cybersicurezza[90]. L'acquisizione della funzione di "punto di contatto unico", prima affidato al DIS, e il trasferimento del CSIRT Italiano presso la sua sede, sono infatti elementi che la portano ad essere parte attiva nei rapporti di cooperazione con l'Agenzia europea per la cybersicurezza (ENISA), con la rete degli CSIRT europei, nonché con il Centro di certificazione europeo e tutte le altre esperienze internazionali nel settore.

Relativamente alla vigilanza, si osserva che l'Agenzia è soggetta a forme di controllo, sia diretto, sia mediato, da parte del COPASIR.

---

[85] art. 12, co. 2, lett. b) nn. 3, 4 e 5 del d.P.C.M. n. 223/2021.
[86] art. 12, co. 2, lett. g) del d.P.C.M. n. 223/2021.
[87] art. 5, co. 3, lett. b) e c) del d.P.C.M. n. 223/2021.
[88] Cfr. art. 7, co. 2, e art. 8, co. 1, del d.P.C.M. n. 223/2021.
[89] art. 11, co. 2, lett. b), c), e), f) del d.l. n. 82/2021.
[90] E. CHITI, *Le agenzie europee. Unità e decentramento nelle amministrazioni europee*, Padova, 2002.

Nel primo caso, ai sensi dell'art. 5 co. 6 del decreto, l'Organo di controllo Parlamentare può chiedere l'audizione del Direttore generale dell'Agenzia su questioni di propria competenza[91], mentre nel secondo caso, l'art. 14 del decreto, dispone che il Presidente del Consiglio dei ministri trasmette una relazione sulle attività svolte dall'Agenzia, rispettivamente, al Parlamento, entro il 30 aprile di ogni anno, nell'abito delle attività svolte al fine di garantire la cybersicurezza nazionale; al COPASIR, entro il 30 giugno di ogni anno, in relazione alle attività svolte «negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del Comitato».

Si evidenzia tuttavia che ulteriori profili di controllo mediato possano essere riscontrati anche nell'obbligo del Presidente del Consiglio di: informare il COPASIR circa la nomina e la revoca del Direttore generale e del Vice Direttore dell'ACN (art. 2, co. 3 del decreto); nel parere positivo delle Commissioni parlamentari competenti, del COPASIR, e il CIC, relativamente all'adozione del regolamento sull'organizzazione e funzionamento dell'Agenzia (art. 6, co. 3, del decreto); nell'adozione del regolamento di contabilità dell'Agenzia, di concerto con il Ministro dell'economia e delle finanze, su proposta del direttore generale dell'Agenzia, previo parere del COPASIR e sentito il CIC (art. 11, co. 3 del decreto); nel parere del CIC sul il bilancio preventivo e il bilancio consuntivo adottati dal direttore generale dell'Agenzia, e nell'invio di tale documento, unitamente alla relaziona annuale, alle Commissioni parlamentari competenti e al COPASIR (art. 11, co. 3, lett. a) e b) del decreto); nel parere del COPASIR e del CIC, sulle procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della cybersicurezza nazionale (art. 11, co. 4, del decreto); nell'obbligo di tempestiva e motivata comunicazione alle Commissioni parlamentari competenti e al COPASIR, dei provvedimenti adottati in materia di dotazione organica dell'Agenzia (art. 12, co. 5, del decreto); ed infine, nel previo parere delle Commissioni parlamentari competenti, del COPASIR e il CIC, sull'adozione del regolamento sull'ordinamento e il reclutamento del personale dell'Agenzia, e il relativo trattamento economico e previdenziale (art. 12, co. 8, del decreto).

Altri profili sono invece legati all'applicazione dell'art. 13, ove è previsto che il trattamento dei dati personali svolto dall'Agenzia avvenga nel rispetto della disciplina sul trattamento dei dati personali per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, di cui alla direttiva (UE) 2016/680 (c.d. direttiva polizia), recepita con il decreto legislativo 18 maggio 2018, n. 51.

[91] L'art. 31 co. 3 della l. 124 del 2007, prevede che il COPASIR, «può altresì 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». Pertanto, si evince che, nonostante l'Agenzia non sia parte del Sistema di informazioni per la sicurezza della Repubblica, il COPASIR svolge funzione di controllo su di essa in quanto deputato alla vigilanza di tutti i soggetti esercenti funzioni di sicurezza nazionale.

Dal rinvio normativo è possibile dedurre che l'ACN sia innanzitutto tenuta a cooperare con l'Autorità garante italiana per la protezione dei dati personali al fine di tutelare i diritti e le libertà fondamentali delle persone i cui dati siano oggetto di trattamento da parte dell'Agenzia[92]; oltre ad essere soggetta al potere di vigilanza dell'Autorità, relativamente alla corretta applicazione della direttiva citata. Si ricorda infatti che l'Autorità garante, nell'esercizio di tale potere, potrà svolgere indagini, ottenere accesso ai dati personali trattati, rivolgere avvertimenti, imporre limitazioni al trattamento, promuovere la segnalazione di violazioni e denunciare i reati commessi[93].

Si precisa tuttavia che tale disposizione debba necessariamente essere interpretata alla luce dei due limiti posti dalla normativa in questione, di cui il primo è quello relativo all'esclusione del potere di controllo dell'Autorità garante sui trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, e di quelle giudiziarie del pubblico ministero; il secondo, attinente invece all'esclusione dall'ambito d'applicazione della direttiva dei trattamenti «effettuati nello svolgimento di attività concernenti la sicurezza nazionale o rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea e per tutte le attività che non rientrano nell'ambito di applicazione del diritto dell'Unione europea»[94]. Sul punto, non può quindi che sorgere un dubbio circa l'applicazione di detta disciplina rispetto alle funzioni svolte dall'Agenzia, considerato che la definizione di "cybersicurezza" fornita dal decreto-legge in questione, dirige espressamente le attività di protezione delle reti e delle risorse informatiche «anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico» (vedi par. 3).

[92] Cfr. art. 7, co. 5 del decreto-legge n. 82 del 2021, ove è previsto che «[n]el rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica», e art. 22 del decreto legislativo 18 maggio 2018, n. 51, ove è previsto che «Salvo quanto previsto dall'art. 37, comma 3, il titolare del trattamento e il responsabile del trattamento cooperano, su richiesta, con il Garante», di cui, secondo certa dottrina, tale disposto deve essere interpretato come un vero e proprio obbligo generale di cooperazione con l'autorità di controllo. Sul punto v. L. BOLOGNINI (diretto da), *Codice della disciplina privacy*, Milano, 2019, p. 774.

[93] Cfr. art. 37 del decreto legislativo 18 maggio 2018, n. 51.

[94] Cfr. art. 1, co. 3, lett. a), b) del decreto legislativo 18 maggio 2018, n. 51. Sul punto preme tuttavia precisare che nonostante l'esclusione dall'ambito applicativo della direttiva polizia dei trattamenti svolti da autorità impegnate nella garanzia della sicurezza nazionale, l'art. 58 del Codice privacy prevede invece che «[a]i trattamenti di dati personali effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, sulla base dell'articolo 26 della predetta legge o di altre disposizioni di legge o regolamento, ovvero relativi a dati coperti da segreto di Stato ai sensi degli articoli 39 e seguenti della medesima legge, si applicano le disposizioni di cui [...] agli articoli 2, 3, 8, 15, 16, 18, 25, 37, 41, 42 e 43 del decreto legislativo 18 maggio 2018, n. 51». La disciplina dettata dal Codice privacy, così come novellato dal d.lgs. 101/2018, estende pertanto la portata applicativa del d.lgs. 18 maggio 2018, n. 51 anche a soggetti che trattano dati personali nell'esercizio di attività di *intelligence*, quali ad esempio il DIS, l'AISE e l'AISI, nonché anche sui trattamenti di dati coperti da segreto di Stato. Per una trattazione più dettagliata sul punto si rinvia a L. BOLOGNINI (diretto da), *op. cit.*, p. 708.

Si conclude infine con i profili della vigilanza interna, rispettivamente attribuiti al Collegio dei revisori dei conti, responsabile del riscontro degli atti della gestione finanziaria su cui formula le proprie osservazioni, nonché delle verifiche di cassa e di bilancio; e all'Organismo indipendente di valutazione (delle performance) – OIV, istituito ed esercente le funzioni di cui all'art. 14, del decreto legislativo 27 ottobre 2009, n. 150.

2.3. Il Nucleo per la Cybersicurezza e i suoi compiti

Il Nucleo per la cybersicurezza è un organismo che trova origine nel c.d. decreto Monti del 2013, il quale lo denominava "Nucleo per la sicurezza cibernetica" (NSC) e lo poneva a supporto del Presidente del Consiglio dei ministri; mentre il decreto Gentiloni del 2017, provvedeva a stabilirne la collocazione presso il DIS.

L'art. 8, comma 1, del decreto-legge in oggetto, dispone invece che il Nucleo sia collocato presso l'ACN, modificandone così anche la sua composizione presidenziale, non più affidata al Vice Direttore del DIS come stabiliva il citato d.P.C.M. 17 febbraio 2013, ma al Direttore generale dell'Agenzia o, per sua delega, al Vice Direttore generale. Resta invece invariata la sua composizione interna, che vede la partecipazione del Consigliere militare del Presidente del Consiglio dei ministri, dei rappresentanti del DIS, dell'AISE, dell'AISI, e di ciascuno dei Ministeri rappresentati nel CIC e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri, salvo diverse integrazioni o formazioni richieste dal decreto per particolari condizioni[95].

Il decreto conferma inoltre la competenza del Nucleo nei profili di "*safety*" essendo chiamato a coordinare, nel rispetto delle proprie competenze, le azioni dei diversi attori che compongono l'architettura istituzionale nelle attività di prevenzione, preparazione e gestione delle eventuali situazioni di "crisi cibernetica"[96], nonché di attivazione delle procedure operative di allertamento.

[95] Cfr. art. 8, co. 3 e 4 del decreto-legge n. 82 del 2021, i quali prevedono che «[i] componenti del Nucleo possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza», e che «[i]l Nucleo può essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi di cui all'articolo 10».

[96] Sula nozione di "crisi cibernetica", sia il d.P.C.M., 24 gennaio 2013 (decreto Monti), sia il d.P.C.M., 17 febbraio 2017 (decreto Gentiloni), definiscono la "situazione di crisi" come «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 ma con l'assunzione di decisioni coordinate in sede interministeriale». Successivamente, all'art. 5, del decreto-legge 21 settembre 2019, n. 105, istitutivo del Perimetro Nazionale di Sicurezza Cibernetica, è stato fatto riferimento alla "crisi di natura cibernetica" come quella condizione di «rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici». A tal proposito, come riferito nel dossier n. 166/2 che ha accompagnato la lettura del citato decreto-legge, il testo originario del disposto faceva espresso richiamo alla definizione di "crisi cibernetica" riportata nei due d.P.C.M., tuttavia, tale richiamo è stato espunto dalla Camera dei deputati in prima lettura del disegno di legge di conversione.

All'art. 9 sono individuati i compiti del Nucleo relativi agli aspetti di prevenzione e preparazione alla crisi cibernetica, consistenti nella partecipazione alla formulazione di proposte per iniziative nazionali e internazionali nel campo della cybersicurezza (lett. a), alla pianificazione di azioni operative di risposta da parte delle amministrazioni pubbliche e degli operatori privati coinvolti in situazioni di crisi cibernetica (lett. b), promuovendo a tal proposito anche esercitazioni interministeriali consistenti nella simulazione di simili eventi (lett. c).

Tuttavia, il tratto essenziale dei compiti affidati all'Organismo interessa certamente la raccolta e valutazione delle informazioni utili ai fini della diffusione degli allarmi relativi agli incidenti di cybersicurezza e alla gestione della crisi.

A tal proposito, il Nucleo promuove innanzitutto, in raccordo con le amministrazioni competenti per specifici profili della cybersicurezza, procedure di condivisione delle informazioni verso i soggetti interessati, sia pubblici sia privati (lett. d), ed allo stesso tempo acquisisce le comunicazioni circa i 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 (lett. e). L'Organismo è quindi posto al centro di una rete di comunicazioni e segnalazioni relative agli incidenti di cybersicurezza provenienti da diversi attori, di cui, primo fra tutti il CSIRT Italiano (lett. f), il CISR, il Comitato scientifico e il DIS, nonché le Forze di polizia, l'organo del Ministero dell'interno di cui all'art. 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, le strutture del Ministero della difesa, le alte amministrazioni che compongono il Nucleo.

Nello specifico, il NC è responsabile della valutazione di tali segnalazioni al fine di verificare se, dimensioni, intensità o natura degli eventi segnalati, siano tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, richiedendo così l'assunzione di decisioni coordinate in sede interministeriale e, qualora tale valutazione abbia esito positivo, il Nucleo provvede ad informare tempestivamente il Presidente del Consiglio dei ministri[97], o l'Autorità delegata, sulla situazione in atto e sullo svolgimento delle attività di raccordo e coordinamento (lett. g).

In altri termini, è il NC a dover valutare e stabilire se l'evento segnalato sia o meno indice di una crisi di cybersicurezza in atto, provvedendo di conseguenza ad attivare la procedura di cui all'art. 10 del decreto.

Al riguardo preme evidenziare che, come specificato nel dossier che ha accompagnato lo studio del decreto da parte delle Camere, in sede di conversione è stato soppresso il comma 2 dell'art. 10, che attribuiva al Nucleo il compito di assicurare il supporto al CISR e al Presidente del Consiglio dei ministri, per gli aspetti relativi la gestione di situazioni di crisi, nonché per l'esercizio dei poteri attribuiti al

[97] Qualora il Presidente del Consiglio dei ministri convochi il CISR al fine di gestire l'evento cibernetico, il comma 1 del decreto dispone che alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'ACN.

Presidente del Consiglio dei ministri, ivi comprese le attività istruttorie e le procedure di attivazione della determinazione del Presidente del Consiglio dei ministri in caso di "crisi di natura cibernetica". La rimozione del suddetto comma lascia quindi intendere che il Legislatore abbia inteso ripartire gli ambiti di intervento in caso di crisi di cybersicurezza, separando l'attività strettamente politica del Presidente del consiglio dei ministri, da quella del Nucleo, di carattere operativo e amministrativo, consistente nella raccolta delle informazioni e coordinamento interministeriale.

La distinzione tra i due piani può essere colta analizzando i commi 1 e 4 dell'art. 10, ove, il primo, dispone che il Presidente del consiglio dei ministri in caso di crisi abbia la facoltà di convocare il CISR in materia di gestione della "crisi cibernetica", integrando le sedute del Consiglio della presenza del Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'ACN[98], mentre il secondo, prevede che in caso di crisi, il Nucleo assicuri che le «attività di reazione e stabilizzazione» di competenza delle diverse amministrazioni ed enti vengano espletate in maniera coordinata.

A tal proposito, si ritiene che al fine di agevolare lo svolgimento di tale compito, si sia preferito integrare la composizione interna del NC. Il comma 3 del disposto prevede infatti che in caso di "crisi cibernetica", la composizione del Nucleo sia rispettivamente integrata, tenendo conto della necessità, della presenza dei rappresentanti del Ministero della salute e del Ministero dell'interno-Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile, in rappresentanza anche della Commissione interministeriale tecnica di difesa civile (CITDC), i quali sono autorizzati ad assumere decisioni che impegnano la propria amministrazione. Inoltre, considerata l'esigenza di un immediato raccordo e maggiore flessibilità in caso di realizzazione di simili eventi, la composizione interna del Nucleo può essere ulteriormente integrata dalla partecipazione dei rappresentanti di altre amministrazioni, anche locali, ed enti, anch'essi autorizzati ad assumere decisioni, e di altri soggetti pubblici o privati eventualmente interessati.

Tuttavia, la funzione primaria di cui è investito il NSC nel ruolo di "gestore" della crisi di cyberiscurezza risulta disciplinata al comma 5 del disposto, ove è previsto che l'organismo «a) mantiene costantemente informato il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla crisi in atto, predisponendo punti aggiornati di situazione; b) assicura il coordinamento per l'attuazione a livello interministeriale delle determinazioni del Presidente del Consiglio dei ministri per il superamento della crisi; c) raccoglie tutti i dati relativi alla crisi; d) elabora rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati; e) partecipa ai meccanismi europei di gestione delle crisi cibernetiche, assicurando altresì i collegamenti finalizzati alla gestione della crisi con gli omologhi

[98] Il disposto riprende la lettera dell'art. 4 del d.P.C.M. Gentiloni, ove al comma 1, lett. a) stabiliva che il CISR «partecipa, in caso di crisi cibernetica, alle determinazioni del Presidente, con funzioni di consulenza e di proposta, nonché di deliberazione nei casi indicati all'art. 7-bis, comma 5, del decreto-legge n. 174 del 2015, convertito con modificazioni dalla legge n. 198 del 2015 [...]». Pertanto, il citato articolo ha di fatto esteso le competenze del CISR anche in ambito di cybersicurezza, nei casi in cui l'evento di crisi sia tale da incidere sulla sicurezza nazionale.

organismi di altri Stati, della NATO, dell'Unione europea o di organizzazioni internazionali di cui l'Italia fa parte».

3. Considerazioni conclusive sulla (cyber)sicurezza nazionale

La nozione di "cybersicurezza" è stata per molto tempo dibattuta tra gli esperti di settore in quanto spesso confusa, o ritenuta intercambiabile, con i due concetti di sicurezza informatica (o *computer security*), e di sicurezza delle informazioni (o *information security*). I recenti interventi legislativi, ed in particolare la nuova normativa, hanno contribuito - seppur in parte[99] - a fare chiarezza sul punto, articolando un'autonoma definizione del concetto.

Difatti, il decreto legge n. 82/2021, che introduce per la prima volta nell'ordinamento italiano la definizione di "cybersicurezza", la descrive come «l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, 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»[100].

La formulazione, frutto di un processo di composizione multidisciplinare, ha il pregio di accogliere al suo interno diversi aspetti caratterizzanti la materia.

Innanzitutto, l'oggetto meritevole di protezione è costituito dalla «disponibilità, confidenzialità e integrità», nonché la «resilienza» delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche; elementi questi che attengono rispettivamente: i primi tre, alle branche della sicurezza informatica e delle informazioni, disciplinate nelle relative normative tecniche di settore[101];

---

[99] Si consideri a tal proposito che il lemma cybersecurity è stato tradotto in alcune normative italiane con il termine "sicurezza cibernetica", non considerando che la cibernetica, quale disciplina che studia l'interazione tra l'uomo e la macchina, non ha alcuna pertinenza – almeno per il momento - con la disciplina della cybersicurezza (o *cybersecurity*).

[100] Cfr. art. 1, co. 1, lett. a) del decreto. La definizione è in linea con quella formulate nel Regolamento (EU) 2019/881, anche noto come "*Cybersecurity Act*", ove all'art. 2, n. 1, il termine "cybersecurity" viene definito «[...] means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats». Più in generale sulle diverse definizioni di cybersicurezza, v. lo studio condotto dall'ENISA raccolto nel documento "*Definition of Cybersecurity. Gaps and overlaps in standardisation*" (il documento è consultabile sul sito dell'ENISA).

[101] La sicurezza delle informazioni è una materia che trova disciplina in diverse norme, sia giuridiche, sia tecniche. Per quanto riguarda le prime, il riferimento è ad esempio, al Regolamento (UE) 2016/679 sulla protezione dei dati personali (c.d. RGPD), al Regolamento (EU) 2018/1807 sul flusso dei dati non personali, ed infine, al complesso di discipline sulla cybersicurezza brevemente tratteggiate in questo scritto. Relativamente alle seconde, la sicurezza delle informazioni è regolata all'interno di normative tecniche che definiscono la corretta implementazione dei c.d. sistemi di gestione della sicurezza delle informazioni (SGSI), ossia l'insieme di politiche, procedure, linee guida, risorse e attività che un'organizzazione, sia essa pubblica o privata, deve implementare per garantire la protezione del proprio patrimonio informativo conformemente a quanto previsto da uno standard certificabile a livello internazionale. Sul punto si ricorda ad esempio la serie di standard ISO/IEC 27000 e seguenti, o anche lo standard statunitense NIST, nonché il *framework* nazionale di cybersicurezza e protezione dei dati personali, elaborato dal Consorzio Interuniversitario Nazionale per l'Informatica (CINI). È ragionevole ritenere che tali norme tecniche abbiano fatto ingresso nell'ordinamento giuridico italiano attraverso i diversi rinvii verso di esse presenti nelle normative (giuridiche) sopraricordate.

quello della resilienza, invece, alla capacità organizzativa del sistema nazionale di prevedere e prevenire gli incidenti di sicurezza informatica che siano tali da mettere in grave crisi il Paese, e di mitigarli qualora questi vadano a segno.

L'art. 1, co. 1, lett. b) del decreto legge, aggiunto in sede di conversione, definisce infatti la "resilienza nazionale nello spazio cibernetico", come l'insieme delle «attività volte a prevenire un pregiudizio per la sicurezza nazionale» che possa comportare un «danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici militari, economici scientifici e industriali dell'Italia, conseguentemente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale [...]»[102].

Ulteriore aspetto, aggiunto anch'esso in sede di conversione, riguarda le finalità delle predette attività poste a «tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico»[103].

Date le brevi premesse, pare possibile innanzitutto cogliere l'ampiezza di questa nuova branca della sicurezza[104], che interessa la protezione dello Stato, sia nel suo complesso istituzionale (Stato-apparato), sia nelle sue specifiche componenti di Stato-collettività, quali la popolazione (società) e le imprese (economia), sintetizzando così in un unico concetto l'insieme delle prospettive giuridicamente rilevanti del diritto alla sicurezza come individuate dalla dottrina gius-pubblicistica sul punto[105]. Caratteristica questa che porta ad evidenziare due aspetti fondamentali: da una parte, la stretta connessione tra la nozione di sicurezza nazionale e quella di ordine e sicurezza pubblica, e dall'altro, la partecipazione attiva delle infrastrutture critiche, composte sia da soggetti pubblici, sia privati, nelle attività di cybersicurezza nazionale.

Relativamente al primo aspetto, la permeabilità degli Stati alle minacce globali, tra cui le minacce informatiche, ha fortemente inciso sui paradigmi securitari, portando ad una interrelazione tra i compiti

---

[102] L'art. 1, co. 1, lett. b) del decreto-legge n. 82/2021, fa espresso rinvio alla lettera dell'art. 1, co. 1, lett. f) del d.P.C.M. 30 luglio 2020, n. 131.

[103] Sul concetto di sicurezza nazionale, v. M. VALENTINI, *L'ordinamento del sistema politico dell'informazione per la sicurezza*, in C. MOSCA – G. SCANDONE – S. GAMBACURTA – M. VALENTINI, *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)*, Milano, 2008, pp. 56; ID, *Sicurezza della Repubblica e democrazia costituzionale. Teoria generale e strategia di sicurezza nazionale*, Napoli, 2017; U. GORI, L. MARTINO, *Intelligence e interesse nazionale*, Roma, 2015; B. VALENSISE, I settori strategici dopo la riforma, in G. DELLA CANANEA, L. FIORENTINO (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Napoli, 2020, pp. 101 ss.; P. CAGGIANO, *Covid-19.Misure urgenti sui poteri speciali dello Stato nei settori della difesa e della sicurezza nazionale, dell'energia, dei trasporti e delle telecomunicazioni*, in *federalismi.it*, 2020.

[104] G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, n. 4, 2019, p. 76.

[105] T.F. GIUPPONI, *Le dimensioni costituzionali della sicurezza*, Bologna, 2010, p. 8, ove l'A. individua le dimensioni giuridiche della sicurezza, tenendo in considerazione alcune prospettive, quali la sicurezza esterna – sicurezza interna; sicurezza individuale (o sicurezza da) – sicurezza collettiva (o sicurezza di); sicurezza materiale – sicurezza ideale. Sul punto v. anche ID., *Le dimensioni costituzionali della sicurezza*, in *forumcostituzionale.it*, 2008; ID., *Sicurezza personale, sicurezza collettiva e misure di prevenzione. La tutela dei diritti fondamentali e l'attività di intelligence*, in *forumcostituzionale.it*, 2008.

di difesa, tradizionalmente volti a proteggere lo Stato dalle minacce esterne, e quelli di sicurezza pubblica, diretta invece ad assicurare la sicurezza interna[106], potendosi così sostenere l'interpretazione di chi ritiene che la «"sicurezza nazionale cibernetica" afferisca all'ambito della pubblica sicurezza, come strumento necessario alla protezione di quegli interessi primari che sono parte essenziale dell'ordine pubblico»[107].

Passando invece al secondo aspetto, strettamente connesso con il primo, si evidenzia che la sicurezza nel cyberspazio pare distinguersi dalla sicurezza "reale" sotto diversi aspetti. A differenza di quest'ultima, infatti, la recente legislazione sulla cybersicurezza, europea e nazionale, presuppone un impegno di tutti gli attori del sistema, comprensivo non solo delle istituzioni pubbliche preposte alle funzioni di sicurezza, ma anche della pubblica amministrazione in generale, delle organizzazioni economiche private, o pubbliche, e soprattutto degli utenti in generale.

Prima che dalla sicurezza dei contenuti in rete, la tutela dei diritti e delle libertà nel cyberspazio, passa per la necessaria messa in sicurezza delle reti e delle risorse informatiche, costituenti a tutti gli effetti un «bene pubblico»[108], che richiede l'impegno, sia dei soggetti detentori di funzioni o servizi essenziali nell'implementare le misure di sicurezza, nonché dei fornitori di progettare, fornire servizi e prodotti ICT c.d. *cybersecurity by design*; sia delle istituzioni di svolgere controlli su tali soggetti e favorire investimenti nel settore supportandone in parte i costi.

Tale interpretazione trova indubbio riscontro nelle due normative cardine accennate in questo scritto, ossia la disciplina NIS e il Perimetro di Sicurezza Nazionale Cibernetica (PSNC), le quali, intervenendo sulla materia con un approccio *all hazzard*, si sono concentrate perlopiù nell'imposizione di controlli sul *procurement* di beni ICT, e nell'obbligo di notifica e segnalazione in caso di incidente informatico a carico dei soggetti che svolgono una funzione o un servizio essenziale per il Paese[109]. Sul punto vi rientra certamente anche l'istituzione dell'Agenzia per la Cybersicurezza Nazionale qui trattata, quale Autorità impegnata nella promozione, sviluppo e finanziamento di specifici progetti ed iniziative nell'ambito della

---

[106] E. CHITI, *Le sfide della sicurezza e gli assetti nazionali ed europei delle forze di polizia e di difesa*, in *Diritto amministrativo*, 2016, p. 545, ove l'A. scrive che «Gli Stati hanno progressivamente ridotto le differenze funzionali tra amministrazione di polizia e amministrazione militare, sempre più chiaramente orientate al perseguimento di un macro-obiettivo comune, quello della tutela della «sicurezza» dell'ordinamento nazionale».

[107] A. MONTI, *Internet e ordine pubblico*, in G. CASSANO – S. PREVITI (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020, p. 78.

[108] Sul concetto di cybersicurezza (o "robustezza dei sistemi" informatici) come bene pubblico v. la recente letteratura gius-economica, M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds & Machines*, in *Springer*, n. 29, 2019; C. MAIOLI, R. BRIGHI, *Sulla cibersicurezza come bene comune*, (il documento è disponibile sul sito del Centro Studi Informatica Giuridica – Osservatorio di Bologna, 23 ottobre 2019; 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*, 8 settembre 2021. In particolare, sull'analisi economia della cybersicurezza v., M.F. GRADY, F. PARISI, *Law and Economics of Cybersecurity*, Cambridge University Press, 2005 e B.H. KOBAYASHI, *An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods*, in *Supreme Court Econoomic Review*, vol.14, 2005.

[109] B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in *federalismi.it*, 13 maggio 2020.

cybersicurezza (di cui alla lett. r dell'art. 7, co. 1 del decreto), oltreché quale Centro nazionale di coordinamento ai sensi dell'art. 6 del regolamento (UE) 2021/887, ed Autorità nazionale di certificazione di cybersicurezza.

Preme tuttavia precisare che i paradigmi securitari dal cyberspazio non interessano solo l'aspetto infrastrutturale (in particolare le vulnerabilità delle reti e delle risorse informatiche), ma riguardano anche gli utenti.

Diversamente dal concetto di sicurezza "reale", la cybersicurezza pone particolare rilevanza non solo verso il profilo esterno, ma anche verso quello della gestione del rischio endogeno che, nel caso specifico, ricomprende gli incidenti di sicurezza dovuti a condotte dolose di soggetti interni ad amministrazioni, organi dello Stato o dipendenti di organizzazioni private, perpetrate con o senza l'ausilio di strumenti informatici[110]; e gli eventi riconducibili al c.d. fattore umano, ossia incidenti dovuti alla mera *inconsapevolezza* degli utenti circa il rispetto di buone pratiche di sicurezza informatica (*best practices*) o sulle tecniche di prevenzione da attacchi di ingegneria sociale[111]. In entrambi i casi, le minacce perpetrate, sebbene spesso circoscritte al solo livello locale, possono facilmente scalare di intensità, al punto da acquisire gradi di compromissione di interesse per la sicurezza nazionale in base alle funzioni, servizi o informazioni colpite. Motivo per cui, oltre al profilo della sicurezza esterna dalle minacce informatiche esogene, acquista prioritario rilievo anche il profilo della sicurezza interna.

Tuttavia, mentre per le condotte malevole perpetrate a mezzo della rete, l'ordinamento provvede alla repressione di tali comportamenti con normative volte a prevenire l'uso distorto delle tecnologie informatiche; nel caso dell'inconsapevolezza degli utenti, si ritiene utile evidenziare che lo Stato italiano è responsabile dell'applicazione di diverse discipline recanti disposizioni sulla promozione di programmi di formazione, sensibilizzazione e istruzione nell'ambito della cybersicurezza al fine di rendere consapevoli gli utenti e diffondere un adeguato grado di cultura della materia presso il pubblico[112].

---

110 G. DE VERGOTTINI, *op. cit*, p. 77. Si tratta dei c.d. *insider threat*, ossia soggetti che sfruttano la propria posizione lavorativa nelle organizzazioni per veicolare attacchi dall'interno. A tal proposito v. M. STRANO, F. BATTELLI, M. BOCCARDI, R. BRUZZONE, B. FIAMMELLA, M. MATTIUCCI, A. RIGONI, *Insiede attack. Manuale di ricerca e di intervento sul computer crime nelle organizzazioni*, Roma, 2005.

111 Per ingegneria sociale (o *social engineering*) si intende «l'uso del proprio ascendente e delle capacità di persuasione per ingannare gli altri, convincendoli che l'ingegnere sociale sia quello che non è oppure manovrandoli. Di conseguenza l'ingegnere sociale può usare la gente per strapparle informazioni con o senza l'ausilio di strumenti tecnologici» (K.D. MITNICK, *L'arte dell'inganno. I consigli dell'hacker più famoso del mondo*, Milano, 2002).

112 Al fine di fornire una panoramica generale sul tema della formazione nell'ambito della cybersicurezza, partendo dal livello internazionale, si faccia riferimento al concetto di «*Awareness*» contemplato nelle risoluzioni dell'Assemblea generale delle Nazioni Unite a partire dal 2003 nell'ambito della «*Creation of a Global Culture of Cybersecurity*», UN doc. A/RES/57/239 (il documento è consultabile sul sito delle Nazioni Unite). A livello europeo, l'art. 4 del Reg. (UE) 2019/881 (c.d. *Cybersecurity Act*), assegna all'ENISA il compito di promuovere «un elevato livello di consapevolezza in materia di cybersicurezza, incluse l'igiene informatica e l'alfabetizzazione informatica, tra cittadini, organizzazioni e imprese», specificato al successivo art. 10 dello stesso Regolamento rubricato «sensibilizzazione e istruzione». Così l'art. 7, par. 1, lett. d), della direttiva NIS, dispone che la strategia nazionale che gli Stati membri sono tenuti a adottare contenga in particolare «un'indicazione di programmi di formazione, sensibilizzazione e istruzione relativi alla strategia

Auspicando pertanto l'organizzazione di simili percorsi a livello nazionale, a partire dagli istituti di formazione quali scuole e università, la questione della (cyber)sicurezza interna porta a dover riflettere sulla titolarità degli utenti a prendere parte a questo genere di iniziative.

Relativamente alle organizzazioni pubbliche e private, sulla spinta del quadro discipline sulla *compliance* (vedi ad esempio il Reg. (UE) 679/2016, relativo alla protezione dei dati personali, e il d.lgs. 8 giugno 2001, n. 231, sulla responsabilità amministrativa degli enti), sono stati recentemente attuati programmi di formazione per il personale interno sulla sicurezza delle informazioni e sulla protezione dei dati personali, sebbene, al momento, tali percorsi formativi costituiscano un obbligo per i soli datori di lavoro e non anche per i dipendenti, diversamente da quanto previsto per i corsi sulla sicurezza sul lavoro[113].

Per quanto riguarda invece la sensibilizzazione dei cittadini, ed in particolare la qualificazione giuridica di simili programmi formativi, pare ragionevole domandarsi se si tratterà di un obbligo, di un dovere o di una facoltà[114]

in materia di sicurezza delle reti e dei sistemi informativi» ed allo stesso modo anche l'art. 6, co. 2, lett. d) del d.lgs. 65/2018, con il quale l'Italia ha recepito la direttiva NIS, ne riproduce il contenuto della disciplina europea. Sul piano nazionale, il già citato art. 7, co. 1, lett. v) e v-bis) del decreto-legge n. 82/2021 attribuiscono all'ACN il compito di promuovere programmi di formazione nel campo della cybersicurezza (in particolare si rinvia al par. 2.2. del presente scritto). L'art. 8 del d.lgs. n. 82/2005 (c.d. Codice dell'Amministrazione Digitale -CAD), rubricato «Alfabetizzazione informatica dei cittadini» dispone che «[l]o Stato e i soggetti di cui all'articolo 2, comma 2, promuovono iniziative volte a favorire la diffusione della cultura digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete, avvalendosi di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo». Inoltre, considerato il costante riferimento delle citate normative europee e nazionali sull'adozione di adeguate misure tecniche e organizzative di sicurezza «tenuto conto delle conoscenze più aggiornate in materia», è opportuno fare riferimento al tema della formazione di cybersicurezza anche nell'ambito delle c.d. norme tecniche richiamate con tale formazione, ossia gli standard internazionali sulla sicurezza delle informazioni. Tra i diversi standard in uso, si faccia riferimento ai punti 7.2. e 7.3 della norma ISO/IEC 27001: 2013, rispettivamente relativi alla "competenza" e "consapevolezza" del personale impiegato nei processi di gestione delle informazioni, nonché al controllo A.7.2.2 dell'Appendice alla norma, attinente alla "consapevolezza istruzione, formazione e addestramento sulla sicurezza delle informazioni".

[113] La recente pronuncia favorevole della Corte di Cassazione sul licenziamento del dipendente che è ingiustificatamente assente al corso di formazione in materia di sicurezza (Cass., civ., Sez. lav., 7 gennaio 2019, n. 138) ha confermato l'obbligo gravante non solo sul datore di lavoro di erogare simili corsi ex d.lgs. 9 aprile 2008, n. 81 e d.lgs. 3 agosto 2009, n. 106, ma anche del lavoratore di prenderne parte.

[114] Cfr. S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2015; L. VIOLANTE, *Il dovere di avere doveri*, Torino, 2014.