dossier

23 luglio 2021

Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale

D.L. 82/2021 – A.C. 3161-A

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Senato della Repubblica

SERVIZIO STUDI
Ufficio ricerche su questioni istituzionali, giustizia e cultura
Ufficio ricerche nei settori infrastrutture e trasporti

TEL. 06 6706-2451 - studi1@senato.it - @SR_Studi

Dossier n. 403/1

Camera dei deputati

SERVIZIO STUDI
Dipartimento istituzioni
Tel. 066760-3855 st_istituzioni@camera.it - @CD_istituzioni

Dipartimento trasporti
Tel. 066760-2614 st_trasporti@camera.it - @CD_trasporti

SEGRETERIA GENERALE – Ufficio Rapporti con l'Unione europea
Tel. 066760-2145 – cdrue@camera.it

SERVIZIO BIBLIOTECA - UFFICIO LEGISLAZIONE STRANIERA
tel. 06/6760. 2278 – 3242 ; mail: LS_segreteria@camera.it

Progetti di legge n. 451/1

D21082a.docx

INDICE

SCHEDE DI LETTURA

Schede di lettura

Premessa

In considerazione dell'accresciuta esposizione alle minacce cibernetiche è emersa negli anni la necessità di sviluppare, in tempi brevi, idonei e sempre più stringenti meccanismi di tutela. Tale esigenza è aumentata negli ultimi anni anche alla luce delle misure volte a garantire infrastrutture *cloud* sicure e centri dati con elevati *standard* di qualità nella direzione di una crescente interoperabilità e condivisione delle informazioni.

A livello di Unione europea la direttiva (UE) 2016/1148 del 6 luglio 2016 reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. **direttiva NIS** - *Network and Information Security*") al fine di conseguire un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea".

La direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 18 maggio 2018, che detta quindi la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS.

Successivamente, il decreto-legge n. 105 del 2019 è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un **perimetro di sicurezza nazionale cibernetica** e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi. Talune modifiche sono state apportate, a tale provvedimento, dal decreto-legge n. 162 del 2019, in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione.

La sicurezza cibernetica costituisce uno degli interventi previsti dal **Piano nazionale di ripresa e resilienza (PNRR)** trasmesso dal Governo alla Commissione europea il 30 aprile 2021.

In tale ambito, la cybersecurity è uno dei 7 investimenti della **Digitalizzazione della pubblica amministrazione**, primo asse di intervento della **componente 1** "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella **Missione 1** "Digitalizzazione, innovazione, competitività, cultura e turismo".

All'investimento, volto alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese a partire dalla attuazione della disciplina prevista dal perimetro di sicurezza nazionale cibernetica, sono destinati circa 620 milioni di euro di cui 241 milioni di euro per la creazione di una infrastruttura nazionale per la cibersicurezza; 231 milioni di euro per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica PSNC; 150 milioni di euro per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'Interno, Difesa, Guardia di Finanza, Giustizia e Consiglio di Stato.

INVESTIMENTO	RISORSE	OBIETTIVO DELL'INTERVENTO	CRONOPROGRAMMA
Cybersecurity (M1C1 I 1.5-5, 6, 7, 8, 9, 20, 21, 22)	**623** (in sovvenzioni) *di cui:* *2021: 170* *2022: 190,4* *2023: 174,0* *2024: 88,6* *2025: --* *2026: --* ▪ 241 infrastruttura cyber; ▪ 231 strutture operative PNSC; ▪ 150 rafforzamento delle capacità difesa informatica di ministeri Interno e Difesa, Guardia di Finanza, Giustizia e Consiglio di Stato	L'investimento è volto alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese a partire dalla attuazione della disciplina prevista dal Perimetro di sicurezza nazionale cibernetica PSNC (su cui si veda *infra*). L'intervento si articola in 4 aree principali: ▪ rafforzamento dei presidi di front-line per la gestione degli alert e degli eventi a rischio verso la PA e le imprese di interesse nazionale; ▪ consolidamento delle capacità tecniche di valutazione e audit della sicurezza dell'*hardware* e del *software*; ▪ potenziamento del personale delle forze di polizia dedicate alla prevenzione e	**Milestones** T4 2022 ▪ istituzione dell'Agenzia per la cibersicurezza nazionale - ACN (disposta con il **D.L. 14 giugno 2021, n. 82)** e adozione del relativo regolamento interno con DPCM ▪ dispiego iniziale dei servizi nazionali di cibersicurezza con la definizione dell'architettura dell'intero ecosistema della cibersicurezza nazionale: un centro nazionale di condivisione e di analisi delle informazioni (ISAC), una rete di squadre di pronto intervento informatico (CERT), un HyperSOC nazionale, il calcolo ad alte prestazioni integrato dagli strumenti di intelligenza artificiale/apprendimento automatico (AI/ML) per analizzare gli incidenti di cibersicurezza di portata nazionale ▪ avvio della rete di laboratori di selezione e

INVESTIMENTO	RISORSE	OBIETTIVO DELL'INTERVENTO	CRONOPROGRAMMA
		investigazione del crimine informatico; implementazione degli asset e delle unità incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber.	certificazione della cibersicurezza ▪ istituzione presso l'ACN di un'unità centrale di *audit* per quanto riguarda le misure di sicurezza PSNC e NIS ▪ sostegno al potenziamento delle strutture di sicurezza: completamento di almeno cinque interventi per migliorare le strutture di sicurezza nei settori PSNC e delle reti e sistemi informativi (NIS) in particolare i settori dell'assistenza sanitaria, dell'energia e dell'ambiente **Target** T4 2024 ▪ dispiego integrale dei servizi nazionali di cibersicurezza: attivazione delle squadre di pronto intervento informatico (CERT), la loro interconnessione con il team italiano di risposta agli incidenti di sicurezza informatica (CSIRT) e con il centro nazionale di condivisione e di analisi delle informazioni (ISAC) e l'integrazione di almeno 5 centri operativi di sicurezza (SOC) con l'HyperSOC nazionale, la piena operatività dei servizi di gestione dei rischi di cibersicurezza, compresi quelli per l'analisi della catena di approvvigionamento e i servizi di assicurazione contro i rischi informatici

INVESTIMENTO	RISORSE	OBIETTIVO DELL'INTERVENTO	CRONOPROGRAMMA
			▪ completamento della rete di laboratori e dei centri per la valutazione e certificazione della cibersicurezza con l'attivazione di almeno 10 laboratori di *screening* e certificazione, dei due centri di valutazione (CV) e attivazione del laboratorio di certificazione UE ▪ piena operatività dell'unità centrale di audit con almeno 30 ispezioni completate

Articoli 1-4
(Architettura nazionale di cybersicurezza)

Gli articoli da 1 a 4 definiscono il **sistema nazionale di sicurezza cibernetica** cha ha al suo vertice il **Presidente** del Consiglio dei ministri cui è attribuita l'alta direzione e la responsabilità generale delle "politiche di cybersicurezza", e a cui spetta l'adozione della relativa strategia nazionale e – previa deliberazione del Consiglio dei ministri - la nomina e la revoca del direttore generale e del vice direttore generale della nuova **Agenzia per la cybersicurezza** nazionale istituita dall'articolo 5 del provvedimento in esame; di tali nomine sono preventivamente informati il **COPASIR** e le competenti **Commissioni parlamentari** (articolo 2).

Il Presidente del Consiglio dei ministri può delegare **all'Autorità delegata** per il sistema di informazione per la sicurezza della Repubblica, ove istituita, le funzioni che non sono a lui attribuite in via esclusiva (articolo 3).

Presso la Presidenza del Consiglio dei ministri è istituito il **Comitato interministeriale per la cybersicurezza (CIC)**, organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cibersicurezza (articolo 4).

Definizioni (articolo 1)

L'**articolo 1, modificato in sede referente,** reca le seguenti definizioni utilizzate nel decreto-legge in esame.

"Cybersicurezza": l'insieme delle attività finalizzate alla tutela delle reti, sistemi informativi, servizi informatici e comunicazioni elettroniche per proteggerli dalle minacce informatiche, assicurando la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini, come specificato dalle Commissioni **in sede referente**, della **tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico**.

Inoltre, sempre nel corso dell'esame in sede referente, sono state fatte salve le attribuzioni di cui alla legge 3 agosto 2007, n. 124 e gli obblighi derivanti da trattati internazionali.

> La legge 124/2007 disciplina il Sistema di informazione per la sicurezza della Repubblica. Questo è composto dal Presidente del Consiglio dei ministri, dal Comitato interministeriale per la sicurezza della Repubblica (CISR), dall'Autorità eventualmente delegata dal Presidente del Consiglio, dal Dipartimento delle informazioni per la sicurezza (DIS), e dai servizi di

informazione: Agenzia informazioni e sicurezza esterna (AISE) e Agenzia informazioni e sicurezza interna (AISI).
Il Comitato parlamentare per la sicurezza della Repubblica (Copasir), composto da cinque deputati e cinque senatori, è l'organo di controllo parlamentare della legittimità e della correttezza costituzionale dell'attività degli organismi informativi (L. 124/2007, artt. 30-38).
Il Presidente del Consiglio dei ministri dirige ed ha la responsabilità generale della politica dell'informazione e della sicurezza (L. 124/2007, art. 1).
Il Comitato interministeriale per la sicurezza della Repubblica (CISR) è organo istituzionale di raccordo politico-strategico sul tema della sicurezza nazionale, con compiti di consulenza, proposta e deliberazione. È presieduto dal Presidente del Consiglio e composto dai ministri degli esteri, dell'interno, della giustizia, della difesa, dell'economia e delle finanze, dello sviluppo economico. Il CISR ha funzioni consultive e di proposta, elabora gli indirizzi generali e gli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza e delibera sulla ripartizione delle risorse finanziarie tra il DIS e i servizi di informazione per la sicurezza e sui relativi bilanci preventivi e consuntivi (L. 124/2007, art. 5).
Il Dipartimento delle informazioni per la sicurezza (DIS) presso la Presidenza del Consiglio ha come compito principale quello di coordinare il complesso delle attività informative e di assicurare l'unitarietà dell'azione dei servizi di informazione per la sicurezza verificando altresì i risultati delle attività svolte da:

- l'Agenzia informazioni e sicurezza esterna (AISE) operante all'estero (L. 124/2007, art. 6);
- l'Agenzia informazioni e sicurezza interna (AISI) che agisce sul territorio nazionale (art. 7).

"Resilienza nazionale nello spazio cibernetico" (definizione introdotta **in sede referente**): le attività volte a prevenire un **pregiudizio alla sicurezza nazionale** nei termini stabiliti dall'articolo 1, comma 1, lettera f*)*, del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131.

Ai sensi della disposizione da ultimo citata per pregiudizio per la sicurezza nazionale si intende 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, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale.

Decreto-legge perimetro: il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.

Decreto legislativo NIS: il decreto legislativo 18 maggio 2018, n. 65, di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione - Direttiva NIS (*Network and Information Security*).

Strategia nazionale di cybersicurezza: la strategia di cui all'articolo 6 del decreto legislativo NIS (vedi *infra* art. 2).

Nel corso dell'esame **in sede referente** sono state apportate inoltre modifiche di carattere formale, sopprimendo le seguenti definizioni e riportando nel testo del decreto-legge le sigle di tali organismi con la loro indicazione per esteso:

- CISR: il Comitato interministeriale per la sicurezza della Repubblica di cui all'articolo 5 della legge 3 agosto 2007, n. 124.
- DIS: il Dipartimento delle informazioni per la sicurezza di cui all'articolo 4 della legge n. 124 del 2007.
- AISE: l'Agenzia informazioni e sicurezza esterna di cui all'articolo 6 della legge n. 124 del 2007.
- AISI: l'Agenzia informazioni e sicurezza interna di cui all'articolo 7 della legge n. 124 del 2007.
- COPASIR: il Comitato parlamentare per la sicurezza della Repubblica di cui all'articolo 30 della legge n. 124 del 2007.

Competenze del Presidente del Consiglio dei ministri (articolo 2)

Il **Presidente del Consiglio dei ministri** è l'autorità al vertice dell'architettura della sicurezza cibernetica, in quanto è a lui attribuita in **via esclusiva** l'**alta direzione e la responsabilità generale** delle politiche di cybersicurezza (**comma 1**). In **sede referente**, è stato soppresso il riferimento alla responsabilità del Presidente del Consiglio ai fini della tutela della sicurezza nazionale nello spazio cibernetico, in quanto tale finalità è ricompresa nella nuova definizione di cybersicurezza (v. *supra*).

Inoltre, al Presidente del Consiglio spetta, sempre in via esclusiva:

- l’adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) istituito all’articolo 4 del presente provvedimento;
- la nomina e la revoca del direttore generale e del vice direttore generale della nuova Agenzia per la cybersicurezza nazionale istituita dall’articolo 5 del provvedimento in esame, previa deliberazione del Consiglio dei ministri, come previsto in sede referente.

Sulle modalità di nomina e revoca dei vertici dell’Agenzia sono intervenute **le Commissioni in sede referente**, prevedendo che il Presidente del Consiglio **informi** preventivamente circa le nomine il **COPASIR** (il decreto-legge faceva riferimento al Presidente di tale organo) e le **Commissioni parlamentari competenti** (**comma 3**).

La definizione della architettura di sicurezza cibernetica si innesta nel contesto istituzionale disciplinato principalmente dal D.Lgs. 65/2018 e dal D.L. 105/2019.
In questa sede occorre ricordare che la **strategia nazionale di sicurezza cibernetica** è un documento previsto dal D.Lgs. 65/2018, di attuazione della direttiva NIS. Ai sensi dell’articolo 6 previgente, il Presidente del Consiglio, previo parere del CISR, adotta la strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale che reca:
- gli obiettivi e le priorità in materia di sicurezza delle reti e dei sistemi informativi;
- 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;
- le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;
- i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;
- i piani di ricerca e sviluppo;
- un piano di valutazione dei rischi;
- l'elenco dei vari attori coinvolti nell'attuazione.

La Presidenza del Consiglio dei ministri trasmette la strategia nazionale alla Commissione europea entro tre mesi dalla sua adozione, escludendo eventualmente la trasmissione di elementi della strategia riguardanti la sicurezza nazionale.
Con la medesima procedura prevista per la strategia nazionale (adozione del Presidente del consiglio previo parere del CISR) sono adottate le linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica.

La disposizione in esame non interviene sui contenuti della strategia nazionale di sicurezza cibernetica, che rimangono disciplinati dal D.Lgs. 65/2018, ma ne muta la denominazione in strategia nazionale di cybersicurezza e provvede a modificarne la procedura di adozione prevedendo il parere del nuovo Comitato interministeriale per la cybersicurezza anziché del CISR (si vedano in proposito anche le puntuali modifiche al D.Lgs. 65/2018 operate in tal senso dall'articolo 15 del provvedimento in esame).

Si anticipa qui quanto previsto dall'art. 4, comma 6, che provvede a trasferire al CIC le funzioni già attribuite al CISR dal decreto-legge 105/2019 e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge 105/2019 (v. *infra*).

Ai sensi del **comma 2**, il Presidente del Consiglio, ai fini dell'esercizio delle competenze di responsabilità generale e dell'attuazione della strategia nazionale di cybersicurezza, impartisce le **direttive per la cybersicurezza** ed emana le **disposizioni per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale**, previo parere del CIC.

Autorità delegata per la cybersicurezza (articolo 3)

L'**articolo 3** prevede che il Presidente del Consiglio dei ministri possa **delegare** all'**Autorità delegata per il sistema di informazione per la sicurezza della Repubblica** (di cui all'articolo 3 della legge n. 124 del 2007), ove istituita, le funzioni che non sono a lui attribuite in via esclusiva (**comma 1**).

Pertanto, non possono essere delegate, in particolare, all'Autorità le funzioni (esplicitamente attribuite in via esclusiva dal comma 1 dell'articolo 2) di alta direzione e responsabilità generale in materia di cibersicurezza, di adozione della strategia nazionale di cybersicurezza e di nomina dei vertici dell'Agenzia.

In caso di nomina dell'Autorità delegata, questa è tenuta a **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 (**comma 2**).

Il Governo attualmente in carica ha provveduto ad istituire l'Autorità delegata per il sistema di informazione per la sicurezza della Repubblica con la nomina del prefetto Franco Gabrielli a Sottosegretario di Stato alla Presidenza del Consiglio. Con il DPCM 8 marzo 2021 (pubblicato nella G.U. 19 marzo 2021,

n. 68) al prefetto Gabrielli è stata conferita la delega per la sicurezza della Repubblica, ai sensi dell'articolo 3 della legge 3 agosto 2007, n. 124.

L'Autorità delegata, in relazione alle funzioni delegate, partecipa alle riunioni del **Comitato interministeriale per la transizione digitale** di cui all'articolo 8 del decreto-legge 1° marzo 2021, n. 22 (**comma 3**).

Il **Comitato interministeriale per la transizione digitale** istituito dal D.L. 22/2021, è la sede di **coordinamento** e **monitoraggio** dell'attuazione delle **iniziative di innovazione tecnologica e transizione digitale** delle pubbliche amministrazioni competenti in via ordinaria.
Sono in ogni caso ricomprese prioritariamente nelle materie di competenza del Comitato interministeriale le attività di coordinamento e monitoraggio circa l'attuazione delle seguenti iniziative:

- strategia nazionale italiana per la banda ultralarga, alle reti di comunicazione elettronica satellitari, terrestri mobili e fisse;
- fascicolo sanitario elettronico e alla piattaforma dati sanitari;
- iniziative per lo sviluppo e la diffusione delle tecnologie emergenti dell'intelligenza artificiale, dell'internet delle cose (IoT) e della *blockchain*.

Le funzioni del Comitato consistono nelle seguenti attività:

- esame delle linee strategiche, attività e progetti di innovazione tecnologica e transizione digitale di ciascuna amministrazione, "anche per valorizzarli e metterli in connessione tra loro in modo da realizzare efficaci azioni sinergiche";
- esame delle modalità esecutive più idonee a fini realizzativi;
- monitoraggio delle azioni e dei progetti in corso, onde verificare lo stato di attuazione delle attività, individuare eventuali disfunzioni o criticità, elaborare possibili soluzioni e iniziative.

Il Comitato è presieduto dal Presidente del Consiglio dei ministri, o, in sua vece, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale, ove nominato, ed è composto da:

- il Ministro per la pubblica amministrazione, ove nominato;
- il Ministro dell'economia e delle finanze;
- il Ministro della giustizia;
- il Ministro dello sviluppo economico;
- il Ministro della salute.

Al Comitato partecipano altresì gli altri Ministri (o loro delegati) aventi competenza nelle materie oggetto dei provvedimenti e delle tematiche poste all'ordine del giorno.
Quando il Comitato tratti materie d'interesse delle regioni e province autonome, alle sue riunioni prendono parte il presidente della Conferenza delle regioni e delle province autonome o un presidente di regione o di

provincia autonoma da lui delegato. Così come partecipano, per i rispettivi ambiti di competenza, il presidente dell'Associazione nazionale dei comuni italiani (ANCI) e il presidente dell'Unione delle province d'Italia (UPI).
È istituita una segreteria tecnico-amministrativa del Comitato, presso la Presidenza del Consiglio, con compiti di supporto e collaborazione, per la preparazione e lo svolgimento dei lavori e per il compimento delle attività di attuazione delle deliberazioni del Comitato.

Comitato interministeriale per la cybersicurezza (articolo 4)

L'articolo 4 istituisce, presso la Presidenza del Consiglio dei ministri, il **Comitato interministeriale per la cybersicurezza (CIC)**, organismo con funzioni di consulenza, proposta e vigilanza in materia di **politiche di cybersicurezza**, (**comma 1**). Anche in questo caso, in **sede referente**, è stato soppresso il riferimento alla responsabilità del Presidente del Consiglio ai fini della tutela della sicurezza nazionale nello spazio cibernetico, in quanto tale finalità è ricompresa nella nuova definizione di cybersicurezza (v. *supra*).

Il **comma 2** attribuisce al CIC i seguenti **compiti**:

- proporre al Presidente del Consiglio gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale;
- esercitare l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza;
- promuovere l'adozione delle iniziative per favorire la collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza;
- esprimere il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale.

La **composizione** del Comitato è stabilita dal **comma 3** come segue:

- il Presidente del Consiglio (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.

Le funzioni di **segretario** del Comitato sono svolte dal **direttore generale dell'Agenzia per la cybersicurezza nazionale** (**comma 4**).

Possono partecipare alle sedute del Comitato, su chiamata del Presidente del Consiglio, anche a seguito di loro richiesta, senza diritto di voto (**comma 5**):

- altri componenti del Consiglio dei ministri;
- altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare.

Nel corso dell'esame in **sede referente** è stata espunta la previsione della partecipazione, sempre su chiamata del Presidente del Consiglio e senza diritto di voto di:

- direttore generale del DIS;
- direttore dell'AISE;
- direttore dell'AISI.

Il **comma 6 trasferisce al CIC** le **funzioni** già attribuite al **CISR** dal decreto-legge 105/2019 (DL perimetro) e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge 105/2019.

Il suddetto articolo 5, nel cui ambito restano in capo al CISR le attuali previsioni, prevede che, in caso di **rischio** grave ed imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, il Presidente del Consiglio, previa deliberazione del **CISR**, può 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.

Per quanto riguarda le altre funzioni in materia di perimetro di sicurezza cibernetica, inizialmente attribuite al CISR e ora **trasferite al CIC** in base al decreto-legge in esame, rientra, in particolare, il compito di proporre al Presidente del Consiglio l'adozione degli atti attuativi (alcuni attuati altri ancora da adottare) del DL 105/2019 (per i quali si veda il paragrafo sul *Quadro normativo*) e di proporre al Presidente del Consiglio l'individuazione dell'elenco (e il suo aggiornamento periodico) dei soggetti inclusi nel perimetro di sicurezza cibernetica (art. 1, comma 2-bis, DL 105/2019).

Oltre alle misure previste dal DL perimetro, sulle competenze poste originariamente in capo al CISR e ora trasferite al CIC interviene altresì l'art. 15 del decreto-legge in esame (si veda *infra*) modificando le previsioni del D.lgs. n. 65/2018 che ha dato attuazione alla direttiva NIS.

Secondo quanto riportato nella relazione illustrativa al decreto-legge, la "scelta di istituire un dedicato Comitato interministeriale, in luogo dell'attribuzione anche delle funzioni in materia di cybersicurezza all'esistente Comitato interministeriale per la sicurezza della Repubblica, risponde ad uno dei richiamati principi ispiratori del presente intervento legislativo, assicurare uno stretto raccordo dell'Architettura di cybersicurezza nazionale con il Sistema dell'intelligence nazionale, a fronte di una chiara separazione di competenze. Si richiama, infatti, che il CISR è uno degli elementi fondamentali del Sistema di informazione per la sicurezza della Repubblica ed è supportato per tutte le funzioni istruttorie dall'organismo informativo di coordinamento, il Dipartimento delle informazioni per la sicurezza (a tale riguardo giova evidenziare che il direttore generale del DIS è il segretario del CISR e presiede l'organo di supporto di cui si avvale il Comitato, il c.d. "CISR tecnico"). La costituzione di un Comitato interministeriale ad hoc, fuori dall'ambito della legge n. 124 del 2007, consentirà altresì all'istituendo Comitato, e all'Agenzia stessa, di muoversi secondo procedure più agili rispetto a quelle adottate dal CISR, chiamato a trattare materie connesse al funzionamento e all'attività degli organismi informativi e connotate, pertanto, e da regimi di elevata classifica di segretezza".

Infine, sul piano meramente redazionale e per il riguardo linguistico, *si valuti l'opportunità di approfondimento riguardo all'utilizzo, in più parti del provvedimento in esame, del vocabolo "cybersicurezza"* (con la lettera "y").

Diversamente il vocabolo "cibersicurezza" (con la i) compare in alcuni atti normativi recenti (quali il D.P.C.M. n. 179 del 2020; la legge n. 53 del 2021, articolo 18) - ovvero si utilizzano perifrasi quali "sicurezza nazionale cibernetica" (cfr. il decreto-legge n. 105 del 2019 e, attuativo, il D.P.C.M. n. 131 del 2020), "sicurezza informatica nazionale" (D.P.C.M.

del 24 gennaio 2013), "protezione cibernetica e sicurezza informatica nazionali" (D.P.C.M. del 2 ottobre 2017).

La circolare per la redazione dei testi legislativi (emanata il 20 aprile 2001 dai Presidenti delle Camere e del Consiglio dei ministri) pone tra le sue raccomandazioni quella di evitare l'uso di termini stranieri, salvo che siano entrati nell'uso della lingua italiana e non abbiano sinonimi in italiano.

L'opzione per il vocabolo con la "i", si ricorda infine, è suggerita dall'Accademia della Crusca, che ha rilevato, in relazione al DL 82/2021, come “l’introduzione di un ibrido italo-inglese come cybersicurezza (calcato sull’inglese *cyber security*) in questo caso, oltre a porre problemi di pronuncia determina anche una incoerenza terminologica che si formerebbe nel corpus legislativo. Si invitano quindi gli organi legislativi a far uso delle risorse della lingua italiana e a ripristinare al suo posto la locuzione “sicurezza nazionale cibernetica” o a sostituirlo con cibersicurezza”.

Articoli 5 e 6, 11 e 12
(Agenzia per la cybersicurezza nazionale)

L'articolo 5 **istituisce l'Agenzia per la cybersicurezza nazionale** a tutela degli interessi nazionali nel campo della cybersicurezza. L'istituzione dell'Agenzia è strumentale all'esercizio delle competenze che il decreto-legge assegna al Presidente del Consiglio dei ministri e all'Autorità delegata, ove istituita (art. 5, comma 2) e svolge in particolare le funzioni e i compiti individuati ai sensi del successivo articolo 7 (si v., *infra*).

Per lo svolgimento dei suoi compiti istituzionali, l'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di rispettiva competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle Forze di polizia o di enti pubblici, nonché delle Forze armate, come precisato nel corso dell'esame in sede referente (art. 5, comma 5).

Il decreto stabilisce che l'Agenzia ha **personalità giuridica** di diritto pubblico ed è dotata di **autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria**, nei limiti di quanto previsto dal decreto in esame (art. 5, comma 2).

In generale, le **agenzie amministrative** rappresentano un modulo organizzativo pubblico per lo svolgimento di attività a carattere tecnico-operativo di interesse nazionale. Generalmente, il ricorso all'agenzia si rende opportuno in presenza di funzioni che richiedano particolari professionalità, conoscenze specialistiche e specifiche modalità di organizzazione del lavoro, più facilmente realizzabili al di fuori delle strutture ministeriali.

Sebbene il modulo organizzativo «agenzia» sia conosciuto in Italia già alla fine degli anni '80 del XX secolo, il d.lgs. n. 300/1999 ha dettato (artt. 8-10) la prima normativa organica sulle agenzie. Tratti distintivi tipici di questa disciplina sono dati dalle condizioni di autonomia in cui le agenzie operano, nei limiti stabiliti dalla legge. Esse dispongono di un proprio statuto; sono sottoposte al controllo della Corte dei conti ed al potere di indirizzo e vigilanza di un ministro; hanno autonomia di bilancio ed agiscono sulla base di convenzioni stipulate con le amministrazioni.

Accanto a questo modello generale, c'è un secondo gruppo di agenzie soggette a una disciplina speciale, derogatoria rispetto a quella del modello generale, ma con caratteristiche giuridiche ed organizzative anche molto diverse tra loro. Tra queste, si ricordano, ad esempio, le c.d. agenzie fiscali, (artt. 10 e 57 ss., d.lgs. n. 300/1999), che includono l'Agenzia delle entrate e l'Agenzia

delle dogane e dei monopoli e sono caratterizzate da una più accentuata autonomia di quella propria delle agenzie del modello generale.

Rispetto a tale contesto, l'Agenzia per la cybersicurezza presenta un carattere speciale, si colloca al di fuori del modello di agenzia creato dal d.lgs. n. 300/1999, le cui disposizioni non vengono richiamate in quanto compatibili e sembrerebbe presentare una più marcata autonomia rispetto ad altre agenzie, a partire dal riconoscimento della personalità giuridica di diritto pubblico, così come avviene per le agenzie fiscali.

Relativamente all'istituzione dell'Agenzia si ricorda che nel corso dell'esame in sede referente è stato eliminato il riferimento alla finalità di tutela della sicurezza nazionale nello spazio cibernetico in quanto tale finalità è ricompresa nella nuova definizione di cybersicurezza di cui all'articolo 1 del provvedimento in esame.

L'Agenzia è disciplinata dalle norme del decreto e dalle fonti alle quali si fa rinvio per gli ulteriori aspetti. In particolare, si ricorda che il decreto-legge prevede l'adozione dei seguenti **regolamenti**:

- regolamento di organizzazione e funzionamento (art. 6, co. 3);
- regolamento di contabilità (art. 11, co. 3);
- regolamento sulle procedure per la stipula di contratti di appalti di lavori e forniture per le attività finalizzate alla sicurezza (art. 11, co. 4);
- regolamento del personale (art. 12, co. 8).

Tutti i citati regolamenti sono adottati, **entro centoventi giorni** dalla data di entrata in vigore della legge di conversione del decreto in esame, con **decreto del Presidente del Consiglio dei ministri**, anche in deroga alle previsioni dell'articolo 17 della legge 23 agosto 1988, n. 400.

Si ricorda che l'articolo 17 della L. n. 400 del 1988 disciplina il potere regolamentare dell'esecutivo, individuando una precisa tipologia dei regolamenti del Governo, riconoscendo la categoria dei regolamenti ministeriali ed interministeriali. La disposizione ha dettato anche una disciplina formale dei regolamenti stabilendo che essi sono adottati con dPR, su deliberazione del Consiglio dei ministri, previo parere del Consiglio di Stato. I regolamenti sono sottoposti al visto e alla registrazione della Corte dei Conti e sono pubblicati in Gazzetta Ufficiale.

Tutti i regolamenti sono adottati **previo parere del Copasir**, sentito il **Comitato interministeriale** per la cybersicurezza, istituito ai sensi dell'articolo 4 del decreto (si v. *supra*); inoltre, come previsto nel corso

dell'esame in sede referente, sugli schemi di regolamento di organizzazione e funzionamento dell'Agenzia (art. 6, co. 3) e di regolamento del personale dell'Agenzia (art. 12, co. 8) è richiesto il **parere delle Commissioni parlamentari competenti, anche per i profili finanziari.** Inoltre, è stato specificato che il parere del **Copasir** è espresso **per i profili di competenza**.

Un'ulteriore disposizione introdotta in sede referente stabilisce che tutti i pareri devono essere resi **entro il termine di 30 giorni** dalla trasmissione dei relativi schemi di decreto. Trascorso inutilmente il termine, si può comunque procedere all'adozione dei relativi provvedimenti (si v. art. 17, co. 10-ter).

In proposito è utile ricordare che il Comitato parlamentare per la sicurezza della Repubblica (**Copasir**), istituito con l'articolo 30 della legge 3 agosto 2007, n. 124 ha la funzione di verificare, in modo sistematico e continuativo, che l'attività del Sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione e delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue istituzioni.

Nell'ambito delle funzioni previste dalla legge al Comitato sono attribuite anche **competenze consultive**. In particolare, l'organo è chiamato a esprimere il proprio parere obbligatorio non vincolante su tutti gli schemi di decreto o di regolamento previsti nella legge di riforma, nonché su ogni altro schema di decreto o di regolamento concernente l'organizzazione e lo stato del personale degli organismi di informazione e sicurezza.

Solo nella procedura di adozione del regolamento di contabilità ed in quello degli appalti è altresì prevista la **proposta da parte del direttore generale dell'Agenzia**.

Organizzazione dell'Agenzia (articolo 6)

L'Agenzia ha sede in Roma ed il regolamento di organizzazione può prevedere l'istituzione di sedi secondarie (art. 6, co. 2, lett. *c)*).

Gli **organi** dell'Agenzia sono costituiti dal direttore generale, che rappresenta l'organo di gestione, e dal collegio dei revisori dei conti, quale organo di controllo interno (art. 5, comma 3 e art. 6, comma 2).

In particolare:

- il **direttore generale** è il legale rappresentante dell'Agenzia ed è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata. Si precisa altresì che egli è "gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia".

A tale ultimo riguardo la previsione è del tutto analoga a quella stabilita per il direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) dall'art. 4, comma 5, della legge n. 124 del 2007.

Il direttore dell'Agenzia è nominato dal Presidente del Consiglio dei Ministri (art. 2, co. 1, lett. c)) ed è **scelto** dallo stesso 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: magistrati delle giurisdizioni superiori ordinaria ed amministrativa, avvocati dello Stato, dirigenti generali dello Stato ed equiparati, professori universitari di ruolo ovvero tra estranei alla pubblica amministrazione. La disposizione richiede altresì il possesso di una **documentata esperienza** di elevato livello nella **gestione dei processi di innovazione**.
L'incarico del direttore ha una **durata massima di 4 anni** e può essere rinnovato per un massimo di ulteriori 4 anni. Il comma 3 dell'articolo 5, a tale riguardo, fa riferimento anche alla figura del **vice direttore generale**, per il cui incarico è stabilita la medesima durata.
Se provenienti dalle pubbliche amministrazioni di cui all'art. 1, co. 2, d.lgs. 165 del 2001, il direttore generale ed il vice direttore sono collocati fuori ruolo o in posizione di comando o altra analoga posizione, secondo gli ordinamenti di appartenenza.
Le **funzioni** del direttore generale e del vicedirettore generale sono disciplinate nel regolamento di organizzazione dell'Agenzia (art. 6, co. 2, lett. *a)*).
Il decreto-legge infine precisa che il **Copasir** "può chiedere **l'audizione**" del direttore generale dell'Agenzia su questioni di propria competenza (art. 5, co. 6), ai sensi di quanto previsto dall'articolo 31, comma 3, della legge 3 agosto 2007, n. 124.

In proposito si ricorda che l'**articolo 31 della L. 124 del 2007** stabilisce che il Copasir, nell'espletamento delle sue funzioni, procede al periodico **svolgimento di audizioni** del Presidente del Consiglio o dell'Autorità delegata, dei Ministri facenti parte del CISR, del direttore generale del DIS e dei direttori di AISE e AISI (comma 1). Il Comitato può ascoltare altresì ogni persona non appartenente al Sistema di informazione per la sicurezza in grado di fornire elementi utili ai fini dell'esercizio del controllo parlamentare (comma 3).

- il **collegio dei revisori dei conti**, di cui non è specificata la composizione, né la durata in carica, ne è indicato a chi ne spetti la

designazione, rinviando per la composizione ed il funzionamento del collegio interamente al regolamento (art. 6, co. 2, lett. b)).

L'Agenzia è articolata in **uffici di livello dirigenziale generale**, che il decreto stabilisce nel numero massimo di **otto** e in **uffici** di livello **dirigenziale non generale**, fino ad un massimo di **trenta** (art. 6, comma 1). In sede referente, è stato precisato che l'articolazione organizzativa è definita nell'ambito delle risorse finanziarie destinate all'Agenzia ai sensi dell'articolo 18, co. 1, del decreto.

Risorse finanziarie e autonomia contabile (articolo 11)

L'articolo 11 detta le disposizioni relative al sistema di finanziamento dell'Agenzia e all'autonomia contabile e gestionale della stessa.

Ai sensi del comma 2 dell'articolo 11, le fonti di **finanziamento** dell'agenzia sono rappresentate da:

- **stanziamenti annuali disposti nella legge di bilancio**, nell'ambito del distinto capitolo istituito ai sensi dell'articolo 18 del decreto in esame presso lo stato di previsione del Ministero dell'economia. Lo stanziamento annuale da assegnare all'Agenzia è stabilito sulla base della determinazione del fabbisogno annuo operata dal Presidente del Consiglio dei ministri e preventivamente comunicata al Copasir (art. 11, comma 1);
- **corrispettivi per i servizi** prestati a soggetti pubblici o privati;
- **proventi** derivanti dallo sfruttamento della **proprietà industriale**, dei prodotti dell'ingegno e delle invenzioni dell'Agenzia;
- **contribuiti dell'Unione europea** o di organismi internazionali, anche derivanti dalla partecipazione a specifici bandi, progetti e programmi di collaborazione;
- **proventi delle sanzioni irrogate** dall'Agenzia ai sensi di quanto previsto dal decreto legislativo NIS, dal decreto-legge perimetro e dal decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;
- **altri** proventi patrimoniali e di gestione e ogni altra eventuale entrata.

A completamento della disciplina, il decreto prevede l'adozione di **due distinti regolamenti** da adottare **su proposta del direttore generale** dell'Agenzia, secondo la procedura già richiamata, *supra*. In particolare:

- il **regolamento di contabilità dell'Agenzia**, volto ad assicurarne l'autonomia gestionale e contabile (art. 11, comma 3). Tale regolamento

può essere adottato anche **in deroga alle norme di contabilità** generale dello Stato e nel rispetto dei principi fondamentali da quelle stabiliti. Tra i principi da rispettare, il regolamento di contabilità deve prevedere che i **bilanci dell'Agenzia**, preventivo e consuntivo, sono adottati dal direttore generale e approvati con dPCm, previo parere del Comitato interministeriale, nonché trasmessi alla Corte dei conti per il controllo preventivo di legittimità. Si dispone inoltre, sulla base delle modifiche approvate in sede referente, che vengano trasmessi al **Copasir** (il decreto-legge faceva riferimento al Presidente di tale organo) e alle **Commissioni parlamentari competenti** il bilancio consuntivo e la relazione della Corte dei conti;

- il **regolamento** (art. 11, comma 4) che definisce le procedure per la stipula dei **contratti di appalti** di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, e in materia di contratti pubblici, ferma restando la disciplina dei contratti secretati di cui all'art. 162 del Codice di cui al D.Lgs. n. 50 del 2016. *Si ricorda in proposito che le disposizioni legislative che prevedono la deroga alle norme in materia di contratti pubblici specificano il necessario rispetto, in particolare, dei vincoli inderogabili derivanti dall'appartenenza all'Unione europea.*

La richiamata disposizione del d.lgs. n. 50 del 2016 stabilisce che le procedure di affidamento possano essere derogate esclusivamente in presenza di due fattispecie:

a) atti ai quali è attribuita una classifica di segretezza;

b) atti la cui esecuzione deve essere accompagnata da speciali misure di sicurezza, in conformità a disposizioni legislative, regolamentari o amministrative.

Per esercitare la deroga, il Codice stabilisce l'obbligo per le Amministrazioni e gli Enti usuari di attribuire, con provvedimento motivato per ciascun procedimento, le classifiche di segretezza, ai sensi dell'art. 42 della legge n. 124 del 2007, ovvero di altre disposizioni in materia. La Corte dei conti, tramite la Sezione centrale per il controllo dei contratti secretati, esercita il controllo preventivo sulla legittimità e sulla regolarità dei contratti in argomento, nonché sulla regolarità, correttezza ed efficacia della gestione. Le risultanze di tale attività conoscitiva confluiscono in un referto presentato, entro il 30 giugno di ciascun anno, al Parlamento.

Per garantire la prima operatività dell'Agenzia nelle more dell'adozione dei due regolamenti citati, si v., *infra*, quanto disposto dall'art. 17, co. 7, del decreto in esame.

Il personale dell'Agenzia (articolo 12)

La **disciplina del personale** addetto all'Agenzia è stabilita in apposito **regolamento** adottato **nel rispetto dei principi generali dell'ordinamento giuridico** e dei criteri indicati nel decreto in esame, anche **in deroga alle vigenti disposizioni di legge**, ivi incluso il Testo unico delle disposizioni in materia di lavoro alle dipendenze della PA, adottato con D.Lgs. n. 165 del 2001.

La deroga è posta in correlazione con le funzioni di tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia.

I tempi e le modalità di adozione del regolamento sono quelle già evidenziate per gli altri regolamenti di disciplina dell'Agenzia (comma 8); in sede referente è stato altresì prevista l'espressione del parere delle **Commissioni parlamentari competenti**, anche per i profili finanziari e del parere del **Copasir** per i profili di competenza.

Il regolamento che definisce l'ordinamento e il reclutamento del personale, nonché il relativo trattamento economico e previdenziale, deve assicurare per il personale di ruolo dell'Agenzia un **trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia**, in base alla "equiparabilità delle funzioni svolte e del livello di responsabilità rivestito".

La specifica normativa regolamentare che attiene al rapporto di impiego della **Banca d'Italia** si sostanzia nei:

- Regolamento del Personale
- Regolamento per il Trattamento di Quiescenza.

I Regolamenti sono adottati dal Consiglio superiore della Banca e recepiscono, nei contenuti, gli accordi negoziali sottoscritti con le Organizzazioni Sindacali presenti all'interno della Banca.

Il **Regolamento del Personale** contiene la normativa in materia di assunzioni, obblighi e divieti, orario, assenze, inquadramento del personale, valutazione e avanzamenti nonché quella in tema di trattamento economico.

Il **Regolamento per il Trattamento di Quiescenza** riguarda sia la previdenza complementare dei dipendenti assunti dal 1993 sia la disciplina previdenziale a esaurimento per il restante personale: i primi hanno la facoltà di aderire al "Fondo pensione complementare per i dipendenti della Banca d'Italia" - gestito dalla Banca stessa - che corrisponde prestazioni pensionistiche calcolate sulla base del complessivo montante contributivo relativo a ciascun aderente.

Tale equiparazione, che l'ultimo periodo del comma 1 riferisce sia al trattamento economico in servizio che al **trattamento previdenziale**, produce effetti avuto riguardo alle anzianità di servizio maturate a seguito dell'inquadramento nei ruoli dell'Agenzia.

In proposito si ricorda che le disposizioni normative che recano un'equiparazione fanno riferimento al trattamento giuridico ed economico del personale e all'ordinamento delle carriere fissati dal contratto collettivo di lavoro in vigore per la Banca d'Italia, che rappresentano il parametro di riferimento per l'ordinamento del personale di alcune autorità indipendenti. È quanto accade per il personale dell'Autorità per la concorrenza e il mercato (AGCM) ai sensi della legge n. 287 del 1990 (art. 11). A sua volta, il trattamento giuridico ed economico del personale delle autorità di regolazione dei servizi di pubblica utilità (Arera e Agcom) è stabilito in base ai criteri fissati dal contratto collettivo di lavoro in vigore per i dipendenti dell'AGCM tenuto conto delle specifiche esigenze funzionali ed organizzative dell'Autorità, ai sensi dell'art. 2, comma 28, della legge n. 481/1995.

In tutti questi casi, le disposizioni legislative fanno riferimento ad un'equiparazione del trattamento giuridico ed economico; la disposizione in esame richiama anche il trattamento previdenziale.

Il regolamento del personale determina in particolare (comma 2):

- l'istituzione di un **ruolo del personale dell'Agenzia** e la disciplina generale del rapporto d'impiego (lett. a), ivi incluse: le ipotesi di incompatibilità (lett. f); le modalità di progressione di carriera all'interno dell'Agenzia (lett. g); la disciplina e il procedimento per la **definizione degli aspetti giuridici e**, limitatamente ad eventuali compensi accessori, **economici del rapporto** di impiego del personale **oggetto di negoziazione** con le rappresentanze del personale (lett. h); i casi di **cessazione** dal servizio del personale a tempo indeterminato ed i casi di anticipata risoluzione dei rapporti a tempo determinato (lett. l); le disposizioni che possono essere oggetto di revisione per effetto della **negoziazione con le rappresentanze** del personale (lett. m);

- la possibilità di procedere, oltre che ad assunzioni a tempo indeterminato attraverso modalità concorsuali, ad **assunzioni a tempo determinato, con contratti di diritto privato**, di soggetti in possesso di alta e particolare specializzazione debitamente documentata, individuati attraverso "adeguate modalità selettive". *Si valuti a tale riguardo l'opportunità di specificare ulteriormente i caratteri e i criteri della selezione.*

- L'assunzione a tempo determinato deve risultare necessaria "per lo svolgimento di attività assolutamente necessarie all'operatività dell'Agenzia o per specifiche progettualità da portare a termine in un arco di tempo prefissato" (lett. b). *In merito andrebbe valutata l'opportunità di chiarire l'espressione "attività assolutamente*

necessarie" al fine di evitare dubbi in sede applicativa, considerato altresì che le assunzioni poste in violazione delle norme del decreto sono nulle ai sensi del successivo comma 6.

- Il regolamento deve inoltre stabilire la **percentuale massima** dei dipendenti che è possibile assumere a tempo determinato (lett. d). In caso di assunzione di professori universitari di ruolo o ricercatori universitari confermati si applicano le disposizioni di cui all'articolo 12 del DPR n. 382 del 1980, anche per quanto riguarda il collocamento in aspettativa (comma 3);

L'art. 12 del DPR 382/1980 disciplina l'autorizzazione ai professori universitari a occuparsi della direzione di istituti e laboratori extrauniversitari di ricerca.

In particolare, prevede che l'autorizzazione è conferita con decreto del Ministro (ora) dell'università e della ricerca, su conforme parere del rettore e del Consiglio del Dipartimento di afferenza e che, in tal caso i professori possono essere collocati, a domanda, in aspettativa. L'aspettativa è concessa con decreto dello stesso Ministro, su parere del Consiglio universitario nazionale (CUN). Se la direzione - ovvero, in base all'interpretazione autentica operata dall'art. 1, co. 2, della L. 118/1989, la presidenza - riguarda istituti o laboratori del Consiglio nazionale delle ricerche e di altri enti pubblici di ricerca il collocamento in aspettativa è con assegni

Durante il periodo dell'aspettativa, ai professori ordinari competono eventualmente le indennità a carico degli enti o istituti di ricerca ed eventualmente la retribuzione ove l'aspettativa sia senza assegni. Il periodo dell'aspettativa è utile ai fini della progressione della carriera e del trattamento di previdenza e di quiescenza. Ai professori collocati in aspettativa è garantita la possibilità di svolgere, presso l'università in cui sono titolari, cicli di conferenze, attività seminariali e attività di ricerca.

- la possibilità di avvalersi di un **contingente di esperti**, non superiore a cinquanta unità, composto da personale **proveniente da pubbliche amministrazioni** *ex* art. 1, co. 2, D.Lgs. 165 del 2001 - con esclusione del personale delle istituzioni scolastiche - ovvero da personale non appartenente alla PA, in possesso di specifici requisiti di competenza e di esperienza indicati dalla norma (lett. c). A tal fine, il regolamento disciplina la composizione del contingente e il compenso spettante per ciascuna professionalità;

- la possibilità di **impiegare personale del Ministero della difesa**, secondo termini e modalità che dovranno essere definite con apposito DPCm (lett. e)*;*

- le modalità di applicazione del Codice della proprietà industriale (D.Lgs. n. 30 del 2005) ai prodotti dell'ingegno ed alle invenzioni dei dipendenti dell'Agenzia (lett. i).

La **dotazione organica** dell'Agenzia, in sede di prima applicazione, è stabilito dal decreto (comma 4) in un **massimo di 300 unità**, così ripartite:

- fino a un massimo di 8 unità di livello dirigenziale generale;
- fino a un massimo di 24 unità di livello dirigenziale non generale;
- fino a un massimo di 268 unità di personale non dirigenziale.

La dotazione organica può essere rideterminata con dPCm, adottato di concerto con il Ministro dell'economia e delle finanze, nei limiti delle risorse finanziarie destinate alle spese per il personale. Dei provvedimenti relativi alla **dotazione organica** è data tempestiva e motivata comunicazione alle **Commissioni parlamentari competenti** e **al Copasir**, come specificato in **sede referente** (comma 5).

In proposito, si anticipa sin d'ora che – nelle disposizioni transitorie e finali - l'art. 17, co. 8, del decreto-legge in esame, in relazione alla fase di prima applicazione del decreto e di avvio dell'Agenzia, prevede l'avvalimento di un nucleo di personale, non superiore al 30 per cento della dotazione organica complessiva iniziale, di unità appartenenti ad altre amministrazioni (si v. *infra*).

Il comma 6 prevede la **nullità delle assunzioni effettuate in violazione** delle disposizioni contenute nel decreto o nel regolamento, ferma restando la responsabilità personale, patrimoniale e disciplinare di chi le ha disposte.

Infine, si dispone un **obbligo del segreto da parte del personale** che presta comunque la propria opera alle dipendenze o in favore dell'Agenzia al rispetto del segreto su ciò di cui sia venuto a conoscenza nell'esercizio o a causa delle proprie funzioni, anche dopo la cessazione di tale attività. In **sede referent**e è stata soppressa la disposizione che faceva salve in ogni caso le classifiche di segretezza che, ai sensi dell'art. 42 della legge n. 124 del 2007, sono attribuite per circoscrivere la conoscenza di informazioni, documenti, atti, attività o cose ai soli soggetti che abbiano necessità di accedervi in ragione delle proprie funzioni istituzionali (comma 7).

Articolo 7
(Funzioni dell'Agenzia)

L'**articolo 7** determina le **funzioni** della "Agenzia per la cybersicurezza nazionale" che il decreto-legge viene a istituire.

Essa è qualificata quale Autorità nazionale, ai fini del complesso di relazioni e funzioni disegnato dalle norme europee ed interne, incluse quelle di certificazione della cibersicurezza.

In tale quadro, predispone in primo luogo la strategia nazionale di cibersicurezza; assume compiti finora attribuiti a diversi soggetti, quali il Ministero dello sviluppo economico, la Presidenza del Consiglio, il Dipartimento delle informazioni e della sicurezza, l'Agenzia per l'Italia digitale; promuove iniziative per lo sviluppo di competenze e capacità.
Presso l'Agenzia sono inoltre trasferiti il **CSIRT italiano** (ora CSIRT Italia: l'acronimo sta per *Computer Security Incident Response Team*) e il Centro di valutazione e certificazione nazionale (**CVCN**).

All'Agenzia sono in particolare attribuite, dall'articolo 7 in esame, le seguenti funzioni:

a) l'Agenzia è Autorità nazionale per la cybersicurezza.

Ne segue che le spetti il coordinamento tra i soggetti pubblici coinvolti nella cibersicurezza a livello nazionale.

Promuove azioni comuni dirette ad assicurare la sicurezza cibernetica, a sviluppare la digitalizzazione del sistema produttivo e delle pubbliche amministrazioni e del Paese, nonché a conseguire autonomia (nazionale ed europea) per i prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore.

Rimane salvo - per le reti, i sistemi informativi ed i servizi informatici attinenti alla gestione delle informazioni classificate - quanto previsto dal regolamento adottato ai sensi della legge n. 124 del 2007 sul "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto" (cfr. il suo articolo 4, comma 3, lettera *l)*; attuativo è il D.P.C.M. n. 5 del 6 novembre 2015, recante "Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva").

Nonché rimangono ferme le competenze dell'Ufficio centrale per la segretezza (istituito entro il Dipartimento delle informazioni per la sicurezza, a sua volta collocato presso la Presidenza del Consiglio: cfr. l'articolo 9 della legge n. 124 del 2007).

Così come rimane fermo che il Ministero dell'interno sia l'autorità nazionale di pubblica sicurezza (come lo designa la legge n. 121 del 1981), titolare delle correlative attribuzioni.

b) "predispone" la **strategia nazionale** di cybersicurezza.

Com'è noto, la strategia nazionale di cibersicurezza - la quale è adottata dal Presidente del Consiglio, sentito il Comitato interministeriale per la sicurezza della Repubblica - è intesa alla tutela della sicurezza delle reti e dei sistemi di interesse nazionale.

Vi sono indicati, tra l'altro, gli obiettivi e le priorità (e la relativa *governance*) in materia di sicurezza delle reti e dei sistemi informativi; i piani di ricerca e sviluppo; un piano di valutazione dei rischi (cfr. l'articolo 6 del decreto legislativo n. 65 del 2018 - l'atto normativo primario che ha dato attuazione alla direttiva (UE) 2016/1148, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione).

c) svolge ogni necessaria attività di **supporto** al funzionamento del "**Nucleo** per la cybersicurezza".

Siffatto Nucleo è istituito dall'articolo 8 del presente decreto-legge, il quale prevede che esso sia presieduto dal direttore generale dell'Agenzia o dal vice direttore da lui delegato.

d) è **Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi**, per le finalità di cui al decreto legislativo n. 65 del 2018, a tutela dell'unità giuridica dell'ordinamento (per le modifiche a tale decreto si veda *infra* l'articolo 15), ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto legislativo.

Si viene pertanto a incidere sul decreto legislativo n. 65 del 2018 (attuativo della direttiva dell'Unione europea n. 1148 del 2016 in materia di sicurezza delle reti e dei sistemi informativi: *Network and Information Security*, donde l'acronimo NIS).

Nella originaria stesura, esso aveva configurato (all'articolo 7) un sistema plurale di autorità competenti NIS per settori (i Ministeri interessati) ed indicato il Dipartimento delle informazioni per la sicurezza quale punto di contatto (ai fini della cooperazione con gli altri Stati membri dell'Unione europea).

La nuova disciplina viene a porre, sopra le autorità di settore, una istanza di raccordo, individuata nella neo-istituita Agenzia, in capo alla

quale è posta la responsabilità dell'attuazione della nuova disciplina posta dal decreto-legge, con titolarità altresì di poteri ispettivi e sanzionatori. La medesima Agenzia diviene il punto di contatto.

e) è **Autorità nazionale di certificazione della cibersicurezza.**

La certificazione di prodotti, servizi, processi delle tecnologie dell'informazione è oggetto di disciplina europea (cfr. artt. 56 e seguenti del regolamento (UE) 2019/881), la quale prevede appunto (all'art. 58) un'autorità nazionale di certificazione.

Essa è ora individuata nell'Agenzia - la quale viene ad assumere tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico, comprese quelle relative all'accertamento delle violazioni ed all'irrogazione delle sanzioni.

Poiché la disciplina europea prevede che solo previo accreditamento da parte dell'organismo nazionale possano operare organismi di valutazione della conformità, si prevede ora che sia l'Agenzia ad accreditare le strutture specializzate del Ministero della difesa e del Ministero dell'interno (quali organismi di valutazione della conformità per i sistemi di propria competenza).

Ancora la disciplina europea prevede che, ove una certificazione della cybersicurezza richieda un livello di affidabilità "elevato", il rilascio di tale certificazione sia effettuabile da un organismo di valutazione della conformità previa delega generale da parte dell'autorità nazionale per la certificazione (oppure dietro sua approvazione di ogni singolo certificato). Si prevede ora che per tali casi l'Agenzia deleghi il Ministero della difesa e il Ministero dell'interno, attraverso le proprie strutture accreditate, al rilascio del certificato europeo di sicurezza cibernetica.

f) assume tutte **le funzioni** in materia di **cybersicurezza** già attribuite dalle disposizioni vigenti al **Ministero dello sviluppo economico**.

Ne segue che siano traslate all'Agenzia le competenze di questo Ministero relative, tra l'altro, al perimetro di sicurezza nazionale cibernetica, alla sicurezza ed integrità delle informazioni elettroniche, alla sicurezza delle reti e dei sistemi informativi.

Per quanto concerne il perimetro di sicurezza nazionale cibernetica - oggetto del decreto-legge n. 105 del 2019 - tale trasferimento di funzioni investe altresì le attività di verifica e ispezione dei privati (attribuite a quel Ministero dall'articolo 1, comma 6, lettera *c)* del decreto-legge n. 105).

Del pari il trasferimento concerne le funzioni attribuite al **Centro di valutazione e certificazione nazionale (CVCN)** presso il Ministero dello sviluppo economico (v. art. 1, comma 6, lettera *a)* del decreto-legge n. 105; e l'articolo 2 del decreto-legge n. 105 aveva autorizzato a quel fine

l'assunzione fino a 77 unità di personale a tempo indeterminato presso il Ministero). Esso viene trasferito dal **comma 4** del presente articolo del decreto-legge presso l'Agenzia. *Si valuti l'opportunità di chiarire se, pur mutando la collocazione dell'organo, restino ferme le norme di organizzazione e funzionamento del Comitato.*

Il **Centro** detiene (ai sensi dell'articolo 1, commi 6 e 7 del decreto-legge n. 105) funzioni incidenti sull'affidamento, da parte dei soggetti rientranti nel perimetro, di forniture di beni, sistemi e servizi ICT (*Information and Communication Technology*) destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici da cui dipenda l'esercizio di una funzione essenziale dello Stato ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, dal cui malfunzionamento, interruzione o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

Per la parte relativa al trasferimento delle funzioni del CVCN si rinvia, altresì, alle disposizioni di cui all'articolo 16, commi 8-10 (v. *infra*).

Circa il perimetro di sicurezza nazionale cibernetica, non rientrano tuttavia tra le **funzioni** trasferite all'Agenzia quelle **spettanti al Ministero per lo sviluppo economico** secondo l'attribuzione resa dall'articolo 3 del D.P.C.M. n. 131 del 2021, recante regolamento in materia di tale perimetro, attuativo del decreto-legge n. 105 del 2019. Quell'articolo 3 prevede che al Ministero per lo sviluppo economico spettino l'individuazione dei soggetti rientranti nel perimetro, in materia di **energia, telecomunicazioni, servizi digitali**.

Per quanto concerne la sicurezza ed integrità delle comunicazioni elettroniche, ad ogni modo, sono novellate (dall'articolo 15 del presente decreto-legge: v. *infra*) le previsioni del Codice delle comunicazioni elettroniche (ossia gli articoli 16-*bis* e 16-*ter* del decreto legislativo n. 259 del 2003, e relative disposizioni attuative) attributive 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. Si intende che tali funzioni divengano di spettanza dell'Agenzia.

Analogo trasferimento concerne la sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo n. 65 del 2018. Talché, ad esempio, è da ritenersi che l'elenco nazionale degli operatori dei servizi essenziali, istituito presso il Ministero per lo sviluppo economico secondo la disposizione previgente, trasli all'Agenzia.

g) partecipa (per gli ambiti di competenza) al **gruppo di coordinamento** istituito dalle disposizioni attuative del decreto-legge n. 21 del 2012, recante norme in materia di **poteri speciali** sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni.

In via attuativa, il regolamento per l'individuazione delle procedure per l'attivazione dei poteri speciali nei settori della difesa e della sicurezza nazionale (a norma dell'articolo 1, comma 8, del decreto-legge n. 21 del 2012), adottato con D.P.R. n. 35 del 2014, ha previsto - ai fini dell'esercizio dei poteri speciali - 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).

h) assume **le funzioni** in materia di **perimetro di sicurezza nazionale cibernetica** attribuite alla **Presidenza del Consiglio**.

Poiché la nuova disposizione menziona "le funzioni", si valuti l'opportunità di approfondire se risulti variata la titolarità dell'atto formale di assunzione delle determinazioni, quando esso sia in capo al Presidente del Consiglio.

Tali funzioni sono individuate dal decreto-legge n. 105 del 2019.

Vi rientrano l'accertamento delle violazioni e l'irrogazione delle sanzioni amministrative, per i soggetti pubblici (nonché i gestori di servizi fiduciari qualificati o di posta elettronica) che facciano parte del perimetro.

Sono però mantenute in capo alla Presidenza del Consiglio le funzioni attribuitegli dall'articolo 3 del citato D.P.C.M. n. 131 del 2021, circa l'individuazione dei soggetti rientranti nel perimetro, per il settore spazio e aerospazio e per il settore tecnologie critiche (e la struttura della Presidenza del Consiglio competente alla innovazione tecnologica e digitalizzazione vi è prevista agire "in raccordo" con il Ministero per lo sviluppo economico, per il settore servizi digitali).

i) assume tutte **le funzioni** già attribuite al **Dipartimento delle informazioni per la sicurezza** dal citato decreto-legge n. 105 del 2019.

Così è da ritenersi che la neo-istituita Agenzia sia chiamata a stabilire misure che garantiscano elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici rientranti nel perimetro, e divenga

destinataria delle notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici.

L'Agenzia in luogo del Dipartimento inoltre è prevista dare ausilio al Presidente del Consiglio dei ministri, a fini di coordinamento dell'attuazione della disciplina del perimetro nazionale.

l) provvede (sulla base delle attività di competenza del "Nucleo per la cybersicurezza" di cui all'articolo 8 del presente decreto-legge: v. scheda *infra*) 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 n. 105 del 2019.

Quest'ultimo articolo richiamato prevede che il Presidente del Consiglio - in presenza di un rischio grave e imminente per la sicurezza nazionale, connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici - possa disporre (su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, e prontamente informando il Comitato parlamentare per la sicurezza della Repubblica) la **disattivazione** (totale o parziale) di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati, secondo un criterio di proporzionalità, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione.

m) assume tutte **le funzioni** in materia di **cibersicurezza** già attribuite all'**Agenzia per l'Italia digitale**.

Tra le disposizioni vigenti, vale ricordare come il Codice dell'amministrazione digitale (decreto legislativo n. 82 del 2005) attribuisse 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 e del Piano nazionale per la sicurezza cibernetica e la sicurezza informatica (cfr. suo articolo 51) nonché l'adozione delle Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione.

Ed altra previgente disposizione (l'articolo 33-*septies*, comma 4, del decreto-legge n. 179 del 2012) attribuiva all'AgID 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*.

Si intende che anche tali compiti spettino ora all'Agenzia.

m-bis) assume le iniziative idonee a valorizzare la **crittografia** come strumento di cibersicurezza - secondo questa **lettera introdotta in sede referente**.

Siffatta valorizzazione della crittografia - ancora prevede la disposizione - può svolgersi anche attraverso un'apposita sezione dedicata della strategia nazionale di ciberiscurezza.

L'Agenzia è prevista attivare, per questo riguardo, ogni iniziativa utile per il 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.

m-ter) provvede alla **qualificazione dei servizi *cloud*** per la pubblica amministrazione - secondo questa **lettera introdotta in sede referente**.

Questa attività è tenuta - aggiunge la disposizione - a rispettare la disciplina dell'Unione europea.

Così come è tenuta al rispetto del regolamento di cui all'articolo 33-*septies*, comma 4, del decreto-legge n. 179 del 2012 - articolo dedicato al consolidamento e razionalizzazione dei siti e delle infrastrutture digitali del Paese; ed il suo comma 4 prevede che l'Agenzia (non più l'AgID, secondo la novella dettata dall'articolo 16, comma 13 del presente decreto-legge, v. *infra)* con proprio regolamento (d'intesa con la competente struttura della Presidenza del Consiglio) stabilisca i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione; definisca inoltre le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi *cloud* per la pubblica amministrazione; individui i termini e le modalità con cui le amministrazioni devono effettuare le migrazioni verso infrastrutture ad alta affidabilità o verso altra infrastruttura propria già esistente in possesso dei requisiti fissati dal medesimo regolamento o verso servizi *cloud*.

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli **incidenti** di sicurezza informatica e gli **attacchi** informatici.

A tal fine l'Agenzia *si avvale* anche del **CSIRT Italia** (previsto dall'articolo 8 del decreto legislativo n. 65 del 2018; cfr. indi il D.P.C.M. 8 agosto 2019, che ne disciplina l'organizzazione), il quale era istituito

presso il Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio - ma il **comma 3** del presente articolo del decreto-legge lo trasferisce presso l'Agenzia.

Si valuti l'opportunità di chiarire se, pur mutando la collocazione dell'organo, restino ferme le norme di organizzazione e funzionamento del Comitato.

L'acronimo CSIRT sta per *Computer Security Incident Response Team* (gruppo di gestione degli incidenti di sicurezza informatica).

I suoi compiti sono: il monitoraggio degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale; la partecipazione alla rete dei CSIRT (che interloquisce con l'Agenzia dell'Unione europea per cibersicurezza).

Secondo una **modifica introdotta in sede referente**, l'Agenzia promuove iniziative di **partenariato pubblico-privato**, onde rendere effettive le ricordate capacità di prevenzione e rilevamento e risposta ad incidenti ed attacchi informatici.

Sulla tassonomia e notifica degli incidenti aventi impatto su beni ICT (l'acronimo sta per *Information and Communication Technology*) cfr. da ultimo il D.P.C.M. n. 81 del 14 aprile 2021.

o) partecipa alle **esercitazioni** nazionali e internazionali in ordine alla simulazione di eventi di natura cibernetica, onde incrementare la "resilienza" del Paese;

p) cura e promuove la definizione ed il mantenimento di un **quadro giuridico** nazionale aggiornato e coerente nel dominio della cibersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale.

"A tal fine, l'Agenzia esprime **pareri** non vincolanti sulle **iniziative legislative o regolamentari**" concernenti la cibersicurezza.

In proposito si valuti l'opportunità di specificare a quali soggetti siano resi tali "pareri", tanto più ove si tratti di "iniziative legislative".

q) coordina, "in raccordo" con il Ministero degli affari esteri e della cooperazione internazionale, la **cooperazione internazionale** nella materia della cibersicurezza.

Per questo riguardo, l'Agenzia cura i rapporti con i competenti organismi dell'Unione europea ed internazionali (salvo che per gli ambiti in cui la legge attribuisca specifiche competenze ad altre amministrazioni;

ma 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).

r) sostiene (negli ambiti di competenza) lo **sviluppo di competenze e capacità industriali, tecnologiche e scientifiche**.

Per questo riguardo l'Agenzia si fa promotrice del coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali.

Può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore.

Ed assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisca competenze in materia di cibersicurezza - in particolare, secondo una modifica introdotta in **sede referente**, con il Ministero della difesa per gli aspetti inerenti alla **ricerca militare**.

Ancora in base ad una modifica introdotta in sede referente, l'Agenzia può altresì 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 cibersicurezza**, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzate a tale scopo".

s) stipula 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 cibersicurezza**. Rimangono ferme le competenze del Ministero degli affari esteri e della cooperazione internazionale.

t) promuove, sostiene e coordina la **partecipazione italiana a progetti e iniziative** dell'Unione europea ed internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali.

Anche in tal caso, è previsto sia assicurato il raccordo con le altre amministrazioni a cui la legge attribuisca competenze in materia di cibersicurezza.

In particolare, secondo quando aggiunge una **modifica introdotta in sede referente**, è assicurato il raccordo con il **Ministero della difesa** per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia Europea per la Difesa.

u) svolge attività di **comunicazione e promozione** della "consapevolezza" in materia di cibersicurezza, "al fine di contribuire allo sviluppo di una cultura nazionale in materia".

v) promuove la **formazione**, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cibersicurezza. Questo, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite **convenzioni con soggetti pubblici e privati**.

Secondo **modifica introdotta in sede referente**, la promozione formativa intrapresa dall'Agenzia è da condursi in particolare favorendo l'**attivazione di percorsi formativi universitari**, in materia di cibersicurezza.

E nello svolgimento dei compiti di promozione della formazione, della crescita professionale e della qualificazione - secondo altra **modifica introdotta in sede referente** - l'Agenzia **può avvalersi** anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno

Le modalità e i termini di siffatto avvalimento sono da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati.

v-bis) può predisporre - secondo questa **lettera introdotta in sede referente** - attività di **formazione** specifica, riservate ai **giovani che aderiscono al servizio civile**.

Tali attività - prosegue la novella disposizione - sono "regolate sulla base di apposite convenzioni" (*non pare maggiormente specificato con quali soggetti esse siano stipulate*).

In ogni caso, **il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile**.

z) può costituire e partecipare a **partenariati pubblico-privato** sul territorio nazionale, nonché (previa autorizzazione del Presidente del Consiglio) a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri.

aa) è **Centro nazionale di coordinamento**, ai sensi del regolamento (UE) 2021/887.

Quel regolamento europeo istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento (e che prevede, all'articolo 6, che ogni Stato membro designi entro il 31 dicembre 2021 un ente che

agisca appunto quale centro nazionale di coordinamento, ai fini dell'attività del Centro europeo).

Il medesimo regolamento europeo prevede che il ricordato Centro europeo di competenza abbia, tra i suoi organi, un consiglio di direzione, composto da un rappresentante per ciascuno Stato membro, il quale ha un supplente (e da due rappresentanti della Commissione europea).

Il **comma 2** del presente articolo del decreto-legge prevede, a tale riguardo, che il rappresentante dell'Italia (ed il suo supplente) entro il consiglio di direzione del Centro europeo siano nominati "nell'ambito dell'Agenzia", con decreto del Presidente del Consiglio.

Una modifica introdotta **in sede referente** aggiunge il **comma 1-*bis***.

Tale disposizioni prevede **l'istituzione di un Comitato tecnico-scientifico**, presso l'Agenzia.

Esso ha funzioni di consulenza e di proposta.

Questo, "anche ai fini dell'esercizio delle funzioni di cui al comma 1, lettere *r), s), t), u), v), z)* e *aa)*".

Tale Comitato è presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato.

Ed è composto da personale della stessa Agenzia nonché da "qualificati" rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza.

Tali componenti sono designati con decreto del Presidente del Consiglio dei ministri.

La composizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo modalità e i criteri da definirsi con il regolamento di organizzazione dell'Agenzia (di cui all'articolo 6, comma 1 del decreto-legge in esame).

Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.

Infine l'Agenzia **consulta il Garante per la protezione dei dati personali** (nel rispetto delle sue competenze, e per le finalità di cui al presente decreto-legge), come prevede il **comma 5** del presente articolo. Consultazione e collaborazione tra Agenzia e Garante - anche in relazione agli incidenti che comportano violazioni di dati personali - possono estrinsecarsi nella stipula di appositi protocolli d'intenti (senza nuovi o maggiori oneri per la finanza pubblica).

Articolo 8
(Nucleo per la cybersicurezza)

L'articolo 8, modificato **in sede referente,** dispone la costituzione, presso l'Agenzia, di un **Nucleo per la cybersicurezza.**

Esso è previsto in via permanente, quale supporto del Presidente del Consiglio riguardo alle tematiche della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

Il Nucleo è presieduto dal **direttore generale dell'Agenzia** o, per sua delega, dal vice direttore generale.

La relativa composizione, sulla base delle modifiche apportate in **sede referente**, è così definita:

- ✓ il Consigliere militare del Presidente del Consiglio;
- ✓ un rappresentante del Dipartimento dell'informazione per la sicurezza (DIS);
- ✓ un rappresentante dell'Agenzia informazioni e sicurezza esterna (AISE) di cui all'articolo 6 della legge n. 124 del 2007;
- ✓ un rappresentante dell'Agenzia informazioni e sicurezza interna (AISI) di cui all'articolo 7 della legge n. 124 del 2007;
- ✓ un rappresentante di ciascuno dei Ministeri rappresentati nel CIC (istituito dall'art. 4 – v. *supra*);
- ✓ un rappresentante del Dipartimento della protezione civile della Presidenza del Consiglio;
- ✓ limitatamente alla trattazione di informazioni classificate, un rappresentante dell'Ufficio centrale per la segretezza (istituito presso il DIS, ai sensi dell'articolo 9 della legge n. 124 del 2007).

I componenti 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 e istituti di ricerca, nonché di operatori privati interessati alla materia della cibersicurezza.

A fronte di questa composizione 'allargata', è prevista una possibile composizione 'ristretta', con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi (sulla quale interviene l'articolo 10 del decreto-legge,

dettando altresì disposizione circa la composizione - in quel caso, integrata con altri esponenti - del Nucleo in situazioni di crisi di natura cibernetica).

La disposizione ‘legifica’ l'istituzione del Nucleo, attualmente previsto dal D.P.C.M. del 17 febbraio 2017, direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, il cui articolo 8 prevede appunto un "Nucleo per la sicurezza cibernetica", presso il Dipartimento delle informazioni per la sicurezza.

Ai componenti del Nucleo non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati, come specificato nel corso dell’esame in **sede referente.**

Articolo 9
(Funzioni del Nucleo)

L'**articolo 9**, modificato in **sede referente,** determina le funzioni (i "compiti", nel dettato della formulazione) del Nucleo per la cyberiscurezza, del quale l'articolo 8 del decreto-legge ha previsto l'istituzione.

Tali funzioni consistono in particolare nelle seguenti attività:

a) formula **proposte** di iniziative in materia di cybersicurezza;

b) promuove (sulla base delle direttive impartite dal Presidente del Consiglio: v. *supra* l'articolo 2, comma 2) la programmazione e la pianificazione operativa, da parte delle amministrazioni e degli operatori privati interessati, della **risposta a situazioni di crisi cibernetica**. Altresì elabora, in raccordo con le pianificazioni di difesa civile e di protezione civile, le procedure di coordinamento interministeriale. La disposizione mantiene fermo l'articolo 7-*bis*, comma 5, del decreto-legge n. 174 del 2015, secondo cui il Comitato interministeriale per la sicurezza della Repubblica può essere convocato dal Presidente del Consiglio dei ministri, con funzioni di consulenza, proposta e deliberazione, in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale;

c) promuove e coordina lo svolgimento **esercitazioni** interministeriali - o la partecipazione italiana ad esercitazioni internazionali - di simulazione di eventi di natura cibernetica;

d) valuta e promuove procedure di **condivisione delle informazioni**, anche con gli operatori privati interessati, ed in raccordo con le amministrazioni competenti, per specifici profili della cybersicurezza, ai fini della **diffusione di allarmi** relativi ad eventi cibernetici e per la gestione delle crisi;

e) secondo quanto specificato nel corso dell'esame in **sede referente** acquisisce, anche per il tramite del CSIRT Italia (su cui v. *supra*, entro la scheda riferita dell'articolo 7 del decreto-legge), 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 del servizi dagli organismi di informazione DIS, AISE e AISI (di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007), dalle Forze di polizia, dall'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (previsto dall'articolo 7-*bis* del decreto-legge n. 144 del 2005), dalle strutture del Ministero della difesa, dalle altre amministrazioni che compongono il Nucleo, dai gruppi CERT di

intervento per le emergenze informatiche (l'acronimo sta per: *Computer Emergency Response Team*);

f) riceve dal CSIRT Italia le **notifiche di incidente** (circa la tassonomia degli incidenti e la loro notifica, cfr. da ultimo il D.P.C.M. n. 81 del 2021);

g) **valuta** se le violazioni (o tentativi di violazione) della sicurezza o i casi di perdita dell'integrità significativi o gli incidenti (di cui alle lettere *e)* e *f)*) assumano **dimensioni, intensità o natura** tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria e da richiedere l'assunzione di **decisioni coordinate in sede interministeriale**. In tal caso il Nucleo provvede ad informare tempestivamente il Presidente del Consiglio (o l'Autorità delegata, ove istituita) sulla situazione in atto e sullo svolgimento delle attività di gestione della crisi (su cui v. *infra* l'articolo 10 del decreto-legge).

Articolo 10
(Gestione delle crisi che coinvolgono aspetti della cybersicurezza)

L'articolo 10, modificato in **sede referente**, disciplina le procedure da seguire per la gestione delle crisi che coinvolgono aspetti di cibersicurezza specificando in particolare i compiti posti in capo al Nucleo per la cibersicurezza istituito ai sensi dell'art. 9 del decreto-legge in titolo.

In particolare, nelle situazioni di crisi che coinvolgono aspetti di cibersicurezza, si prevede che - nei casi in cui il Presidente del Consiglio dei ministri convochi il Comitato interministeriale per la sicurezza della Repubblica (CISR) in materia di gestione delle predette situazioni di crisi – siano chiamati a **partecipare alle sedute del CISR**:

- il Ministro delegato per l'innovazione tecnologica e la transizione digitale;
- il direttore generale dell'Agenzia.

Nel corso dell'esame in sede referente è stata soppressa la previsione (comma 2) che attribuiva al Nucleo il compito di assicurare il supporto al CISR e al Presidente del Consiglio dei ministri, nella materia della cibersicurezza, per gli aspetti relativi alla suddetta gestione di situazioni di cris, nonche' per l'esercizio dei poteri attribuiti al Presidente del Consiglio dei ministri, ivi comprese le attivita' istruttorie e le procedure di attivazione necessarie, ai sensi dell'articolo 5 del decreto-legge n. 105/2019 sul perimetro.

Relativamente alla **composizione del Nucleo**, si prevede, tenuto conto delle modifiche approvate in sede referente, che in situazioni di **crisi di natura cibernetica** il Nucleo sia **integrato**, in ragione della necessità, con un rappresentante, rispettivamente:

- del Ministero della salute;
- 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.

Tali rappresentanti sono autorizzati ad assumere decisioni che impegnano la propria amministrazione. Inoltre, si dispone che alle riunioni i componenti possano farsi accompagnare da altri funzionari della propria amministrazione.

Alle medesime riunioni possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, e di altri soggetti pubblici o privati eventualmente interessati.

Per la partecipazione non sono previsti compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

Al Nucleo è affidato il compito, nella composizione per la gestione delle crisi, di assicurare che "le **attività di reazione e stabilizzazione**" di competenza delle diverse amministrazioni ed enti rispetto a situazioni di crisi di natura cibernetica, vengano espletate in maniera coordinata secondo quanto previsto dall'articolo 9, comma 1, lettera b) che attribuisce al Nucleo il compito di promuovere, sulla base delle direttive, la programmazione e pianificazione operativa della risposta a situazioni di crisi cibernetica.

In base al comma 5, il **Nucleo**, per l'espletamento delle proprie funzioni:

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

Resta fermo quanto previsto ai sensi dell'articolo 7-*bis*, comma 5, del decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015, che stabilisce che il CISR possa essere **convocato** dal Presidente del Consiglio dei ministri, con funzioni di **consulenza, proposta e deliberazione**, in caso di situazioni di crisi che coinvolgano aspetti di **sicurezza nazionale**.

Articolo 13
(Trattamento dei dati personali)

L'articolo 13 prevede che i trattamenti di dati personali per **finalità di sicurezza nazionale**, in applicazione del decreto legge in esame, siano effettuati ai sensi del **Codice in materia di protezione dei dati personali,** con particolare riguardo alle specifiche disposizioni previste per finalità di difesa o di sicurezza dello Stato.

In particolare, l'articolo 13 richiama l'articolo 58, commi 2 e 3, del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) concernenti i trattamenti di dati personali per fini di sicurezza nazionale o difesa.

Il richiamato art. 58, comma 2, del Codice dispone che, ai trattamenti **effettuati da soggetti pubblici per finalità di difesa o di sicurezza** dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, si applicano:

- le disposizioni (di cui al comma 1, del medesimo art. 58) concernenti i **controlli** relativi ai trattamenti di dati personali effettuati dagli **organismi** previsti dalla legge 3 agosto 2007, n. 124 (DIS, AISE e AISI) e **di dati coperti da segreto di Stato**; in base a tali disposizioni (tramite il richiamo all'art. 160, comma 4 del Codice privacy) il componente designato per gli accertamenti dal Garante per la protezione dei dati personali deve prendere visione degli atti e dei documenti rilevanti e riferire oralmente nelle riunioni del Garante;

Si ricorda che, ai sensi dell'art. 158 del Codice, il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali. L'art. 160 dispone che, **per i trattamenti di dati personali di cui all'articolo 58, gli accertamenti sono effettuati per il tramite di un componente designato dal Garante** e che non sono delegabili. La disposizione specifica inoltre che quando risulta necessario in ragione della specificità della verifica, il componente designato può farsi assistere da personale specializzato tenuto al segreto e che gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza. Il comma 4 dell'art. 160 richiamato in commento dispone che, per gli accertamenti relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente appositamente designato dal Garante prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante stesso.

- le disposizioni concernenti la **valutazione d'impatto** sulla protezione dei dati e la **consultazione preventiva del Garante**, di cui agli articoli

23 e 24 del decreto legislativo 18 maggio 2018, n. 51, concernente il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali; nonché, in quanto compatibili, specifiche ulteriori disposizioni contenute nel medesimo decreto legislativo n. 51.

Si ricorda che il decreto legislativo 18 maggio 2018, n. 51, che reca attuazione della direttiva (UE) 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. In particolare l'articolo 23 prevede che se il trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, prima di procedere al trattamento, effettua una valutazione del suo impatto sulla protezione dei dati personali, la quale contiene una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e il rispetto delle norme del presente decreto. L'art. 24 prevede invece che il titolare del trattamento o il responsabile del trattamento consultino il Garante prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se: una valutazione d'impatto indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure il tipo di trattamento presenti un rischio elevato per i diritti e le libertà degli interessati anche in ragione dell'utilizzo di tecnologie, procedure o meccanismi nuovi ovvero di dati genetici o biometrici.
Le ulteriori disposizioni del D.lgs. 51/2018 richiamate sono quelle relative alle definizioni (art. 2), ai principi applicabili (art. 3), al processo decisionale automatizzato relativo alle persone fisiche (art. 8), agli obblighi del titolare del trattamento (art. 15), alla protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 16), al responsabile del trattamento (art. 18), alla sicurezza del trattamento (art 25), all'Autorità di controllo (art. 37), al diritto al risarcimento (art. 41), alle sanzioni amministrative (art. 42) e al trattamento illecito di dati (art. 43).

L'articolo in esame richiama infine il comma 3 dell'art. 58 del Codice privacy, il quale demanda ad uno o più **regolamenti** l'individuazione delle **modalità di applicazione**, in riferimento alle tipologie di dati, di interessati, di **operazioni di trattamento eseguibili e di persone autorizzate** al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, anche in relazione all'aggiornamento e alla conservazione.

Il comma 3 dell'art. 58 prevede altresì che i suddetti regolamenti, in base agli ambiti di intervento, sono adottati ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto) o con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su proposta dei Ministri competenti.

Articolo 14
(Relazioni al Parlamento)

Al **Parlamento** deve essere trasmessa, ai sensi dell'art. 14, comma 1, una relazione entro il 30 aprile di ogni anno sull'**attività svolta** dall'Agenzia nell'anno precedente in materia di cybersicurezza nazionale.

Nel corso dell'esame in **sede referente** è stato previsto – tra le disposizioni finali - che la prima relazione al Parlamento (di cui all'articolo 14, comma 1) venga trasmessa entro il **30 novembre 2022**.

Inoltre, è stato aggiunto che entro il **31 ottobre 2022** il Presidente del Consiglio dei ministri è tenuto a trasmettere al Parlamento una relazione che dia conto dell'attuazione al 30 settembre 2022 delle disposizioni di cui al decreto-legge in esame, anche al fine di formulare eventuali proposte in merito.

In base all'articolo 14, comma 2, il Presidente del Consiglio dei ministri è tenuto a **trasmettere** al Comitato parlamentare per la sicurezza della Repubblica (**COPASIR**) – **entro il 30 giugno** di ogni anno - una **relazione** che, secondo quando specificato in **sede referente**, verta sulle attività svolte nell'anno precedente dall'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del COPASIR.

Relativamente agli **ambiti di attività dell'Agenzia** sottoposti al **controllo del COPASIR** ai sensi del decreto-legge in esame, come modificato in **sede referente**, si ricorda, in particolare, che:

- il Presidente del Consiglio dei ministri informa preventivamente il COPASIR e le Commissioni parlamentari competenti riguardo alla **nomina e alla revoca del direttore generale e del vice direttore** generale dell'Agenzia per la cybersicurezza nazionale (art. 2, comma 3);
- il COPASIR può chiedere **l'audizione del direttor generale** dell'Agenzia su questioni di propria competenza, ai sensi di quanto previsto dall'articolo 31, comma 3, della legge 3 agosto 2007, n. 124 (art. 5, comma 6);
- il COPASIR – nonché Commissioni parlamentari competenti, anche per i profili finanziari - esprime il **parere, per i profili di competenza,** sul regolamento di **organizzazione** dell'Agenzia (art 6);
- con legge di bilancio è determinato lo **stanziamento annuale** da assegnare all'Agenzia sulla base della determinazione del fabbisogno annuo operata dal Presidente del Consiglio dei ministri, previamente comunicata al COPASIR (art. 11);

- il **regolamento di contabilità dell'Agenzia**, è adottato con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, su proposta del direttore generale dell'Agenzia, previo parere del COPASIR e sentitoil CIC (art. 11);
- il **bilancio consuntivo** e **la relazione della Corte dei conti** sono trasmessi al COPASIR (art. 11), nonché alle Commissioni parlamentari competenti;
- con regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta del direttore generale dell'Agenzia, previo parere del COPASIR e sentito il CIC, sono definite le **procedure per la stipula di contratti di appalti di lavori e forniture di ben e servizi** per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico (art. 11);
- con decreti del Presidente del Consiglio dei ministri di concerto con il Ministro dell'economia e delle finanze, la **dotazione organica** può essere rideterminata nei limiti delle risorse finanziarie destinate alle spese per il personale. Dei provvedimenti adottati in materia di dotazione organica dell'Agenzia è data tempestiva e motivata comunicazione alle Commissioni parlamentari competenti e al COPASIR (art. 12);
- il **regolamento sul personale** è adottato, previo parere del COPASIR per i profili di competenza, nonché previo parere delle Commissioni parlamentari competenti, anche per i profili finanziarie e sentito il CIC (art. 12);
- il direttore generale dell'Agenzia, fino all'adozione dei regolamenti di cui all'articolo 11, identifica e assume gli **impegni di spesa** che verranno liquidati a cura del DIS, nell'ambito delle risorse destinate all'Agenzia. Entro 90 giorni dall'approvazione dei regolamenti di cui all'articolo 11, delle spese così effettuate il Presidente del Consiglio dei ministri ne dà informazione al COPASIR (art. 17).

Articolo 15
(Modifiche al D.Lgs. 65/2018, c.d. decreto NIS)

L'articolo 15, modificato in **sede referente**, modifica il decreto legislativo n. 65 del 2018 che ha dato attuazione alla direttiva (UE) 2016/1148 ***(c.d.*** **direttiva** ***Network and Information Security*** - NIS), tenendo conto della nuova architettura delineata dal decreto-legge in esame. Tale decreto legislativo rappresenta la cornice legislativa delle misure per la sicurezza delle reti e dei sistemi informativi e dei soggetti competenti a dare attuazione agli obblighi previsti in tale ambito.

La **direttiva (UE) 2016/1148** del 6 luglio 2016 ha previsto misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione al fine di conseguire un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea".

Le modifiche recate dall'art. 15 sono volte ad **adeguare il decreto legislativo n. 65 del 2018** alle previsioni del **decreto-legge** in esame.

Il decreto legislativo n. 65/2018 ha dettato le misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva 2016/1148.

In particolare tale provvedimento – nel testo in vigore prima del decreto-legge in esame – prevede che al **Presidente del Consiglio dei ministri** compete l'adozione, sentito il Comitato interministeriale per la sicurezza della Repubblica (**CISR**), della strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Con la medesima procedura sono adottate linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica.

La qualifica di **autorità competente NIS** viene attribuita ai singoli ministeri in base ai settori di competenza (Ministero dello sviluppo economico, Ministero dell'economia e delle finanze, Ministero della salute e Ministero dell'ambiente e della tutela del territorio) e, per taluni ambiti, alle regioni e alle province autonome di Trento e di Bolzano. Tali autorità sono i soggetti competenti per settore (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali) in materia di sicurezza delle reti e dei sistemi informativi; verificano, in particolare, l'applicazione della direttiva a livello nazionale ed individuano gli operatori di servizi essenziali nell'ambito dei criteri ivi definiti.

Presso la Presidenza del Consiglio dei ministri è istituito il **CSIRT-***Computer Emergency Response Team* italiano, con un contingente di 30 persone e lo stanziamento di specifiche risorse finanziarie, al quale sono attribuite – a

decorrere dall'entrata in vigore del relativo decreto di organizzazione e funzionamento - le funzioni del CERT nazionale (attualmente presso il Ministero per lo sviluppo economico) e del CERT-PA (attualmente presso l'Agenzia per l'Italia digitale-AGID). Il CSIRT è definito dalla direttiva 2016/1148 quale "gruppo di intervento per la sicurezza informatica in caso di incidente", che ogni Stato membro è chiamato a designare con il compito di trattare gli incidenti e i rischi secondo una procedura definita.

Viene designato il Dipartimento delle informazioni per la sicurezza (DIS) quale **punto di contatto unico**, organo incaricato a livello nazionale di coordinare·le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea.

L'**autorità di contrasto** è individuata nell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione al quale è attualmente attribuita la competenza ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

Gli **operatori di servizi essenziali**, ai fini del provvedimento, sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), individuati dalle autorità competenti NIS.

Il decreto definisce inoltre gli **obblighi** in capo agli **operatori dei servizi essenziali e ai fornitori dei servizi digitali** con riferimento alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall'allegato III. È posto a loro carico l'obbligo di individuare le misure tecniche e organizzative relative alla gestione dei rischi, alle misure per prevenire e minimizzare gli impatti degli incidenti e, sotto il profilo procedurale, sono definite le modalità di notifica degli incidenti che abbiano un impatto rilevante sui servizi forniti individuando altresì le condizioni e le modalità secondo le quali potranno essere coinvolti gli organismi di altri Paesi.

Sono poi individuati i **poteri di controllo delle autorità NIS** sia nei confronti degli operatori di servizi essenziali, che dei fornitori di servizi digitali anche prevedendo poteri di verifica e di ispezione oltre che l'irrogazione di sanzioni amministrative nel caso di mancato adempimento degli obblighi previsti.

In primo luogo, i riferimenti alle autorità nazionali competenti sono sostituiti con quelli all'**autorità nazionale competente NIS**, in considerazione dell'istituzione dell'Agenzia da parte del decreto-legge in esame, e alle autorità di settore.

Il decreto-legge n. 82 del 2021 in esame, nel ridefinire l'architettura italiana di cybersicurezza, prevede – come evidenziato nelle premesse del provvedimento - l'istituzione di un'apposita Agenzia per la cybersicurezza nazionale "per adeguarla all'evoluzione tecnologica, al contesto di minaccia

proveniente dallo spazio cibernetico, nonché al quadro normativo europeo", e raccorda le disposizioni in materia di sicurezza delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche.

A seguito delle modifiche apportate dal decreto-legge in esame i richiami del d. lgs. 65/2018 alla strategia nazionale di sicurezza cibernetica sono dunque riferiti alla "**strategia nazionale di cybersicurezza"**.

Vengono specificate quindi le modalità per il riesame e l'aggiornamento dell'**elenco degli operatori di servizi essenziali** sulla base delle competenze poste in capo alla istituenda Autorità specificando che le autorità di settore, in relazione ai settori di competenza, propongono all'**autorità nazionale competente NIS** le variazioni all'elenco degli operatori dei servizi essenziali, secondo i criteri previsti dalla legge; le proposte sono valutate e, come specificato in **sede referente**, eventualmente integrate, d'intesa con le autorità di settore, dall'autorità nazionale competente NIS che, con propri provvedimenti, provvede alle variazioni dell'elenco degli operatori dei servizi essenziali, dandone comunicazione, in relazione ai settori di competenza, anche alle autorità di settore.

Sempre in considerazione della nuova architettura delineata dal decreto-legge in esame sono sostituiti, nel settore della sicurezza cibernetica, i riferimenti al Comitato interministeriale per la sicurezza della Repubblica (CISR) con quelli al **Comitato interministeriale per la cybersicurezza (CIC)**. In primo luogo, si prevede che il Presidente del Consiglio dei ministri adotti, sentito il CIC – anziché sentito il CISR – "la strategia nazionale di cybersicurezza per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale".

Spetta inoltre all'istituenda Agenzia trasmettere alla Commissione europea la **strategia nazionale** in materia di cybersicurezza entro tre mesi dalla sua adozione (trasmissione in precedenza posta in capo alla Presidenza del Consiglio dei ministri).

Sono quindi coordinati i riferimenti alle autorità di settore – in precedenza designati autorità NIS – con il riferimento all'Agenzia per la cybersicurezza nazionale, designata – come detto - quale **autorità nazionale competente NIS** a cui si accompagni la designazione, quali **autorità di settore**, dei competenti **ministeri** in base ai settori di riferimento (energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, infrastrutture digitali, fornitura e distribuzione acqua potabile) e delle **regioni e province autonome** in considerazione degli ambiti di competenza.

Viene specificato che l'autorità nazionale competente NIS è **responsabile dell'attuazione** delle misure previste dal decreto

legislativo n. 65/2018 con riguardo ai settori e servizi ivi elencati (allegato II e allegato III) e ad essa spetta la **vigilanza** sull'applicazione del decreto a livello nazionale, incluso l'esercizio delle relative **potestà ispettive e sanzionatorie**.

L'Agenzia per la cybersicurezza nazionale è designata inoltre quale **punto di contatto unico** in materia di sicurezza delle reti e dei sistemi informativi, mentre in precedenza tale ruolo era svolto dal DIS.

Il punto di contatto unico svolge, in particolare, una funzione di collegamento per garantire la **cooperazione transfrontaliera** dell'autorità nazionale competente NIS con le autorità competenti degli altri Stati membri, nonché con il gruppo di cooperazione e la rete di CSIRT.

L'Agenzia per la cybersicurezza nazionale, in qualità di autorità nazionale competente NIS e di punto di contatto unico **consulta**, conformemente alla normativa vigente, l'autorità di contrasto ed il Garante per la protezione dei dati personali e **collabora** con tali organismi.

Viene inoltre previsto che il **CSIRT italiano**, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale operi **presso l'istituenda Agenzia** anziché presso la Presidenza del Consiglio dei ministri - Dipartimento delle informazioni per la sicurezza.

Ai sensi del nuovo art. 9 del d. lgs. N. 65/2018 le autorità di settore collaborano con l'autorità nazionale competente NIS per l'adempimento degli obblighi di al medesimo decreto. A tal fine il **Comitato tecnico di raccordo** opera **presso l'Agenzia** per la cybersicurezza nazionale, anziché presso la Presidenza del Consiglio dei ministri.

Si specifica, con le modifiche apportate, che il Comitato tecnico di raccordo "è presieduto dall'autorità nazionale competente NIS".

Il **Comitato tecnico di raccordo** è composto dai rappresentanti delle amministrazioni statali "individuate quali **autorità di settore**" secondo la nuova architettura definita dal provvedimento in esame e da rappresentanti delle **regioni e province autonome** in numero non superiore a due, secondo quanto già previsto dal d.lgs. 65/2018.

Per quanto riguarda le procedure di **notifica** degli incidenti, di cui all'art. 14 del d.lgs, 65/2018, si prevede che i fornitori di servizi digitali **notifichino al CSIRT italiano** (e non più, per conoscenza, all'autorità competente NIS) senza ingiustificato ritardo, **gli incidenti** aventi un

impatto rilevante sulla fornitura di un servizio (di cui all'allegato III del decreto n. 65) che essi offrono all'interno dell'Unione europea.

Talune modifiche ed integrazioni sono inoltre previste all'Allegato I del d. lgs. 65/2018 con riguardo all'attività del CSIRT.

Infine, come già ricordato, l'**autorità nazionale competente NIS** – in luogo delle singole autorità di settore - è competente per l'accertamento delle violazioni e per l'irrogazione delle **sanzioni amministrative** previste dal decreto legislativo n. 65/2018 (art. 19) e allo svolgimento delle attività di ispezione e verifica necessarie per le misure previste dal medesimo decreto legislativo in particolare in materia di sicurezza e notifica degli incidenti.

È soppressa, in tale ambito, la previsione (art. 19, co. 2) che demandava ad un successivo Accordo tra Governo, Regioni e Province autonome di Trento e di Bolzano la definizione di criteri uniformi in ambito nazionale per lo svolgimento delle attività di ispezione e verifica, necessarie per le misure previste dagli articoli 12, 13, 14 e 15, che riguardano le reti e i sistemi informativi utilizzati dagli operatori che prestano attività di assistenza sanitaria, nonché in merito al settore fornitura e distribuzione di acqua potabile.

Infine, l'articolo 15 specifica che nel decreto legislativo n. 65/2018 ogni riferimento al Ministero dello sviluppo economico deve intendersi riferito all'Agenzia per la cybersicurezza nazionale, fatta eccezione per le disposizioni di cui all'articolo 7, comma 1, lettera a), del medesimo decreto legislativo che, come detto, designano il Ministero dello sviluppo economico quale autorità di settore per quello delle infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali.

Ogni riferimento al DIS deve intendersi riferito all'Agenzia per la cybersicurezza nazionale e ogni riferimento alle autorità competenti NIS, deve intendersi riferito all'autorità nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo che riguarda le procedure per gli effetti negativi rilevanti.

Di seguito sono illustrate, con un **testo a fronte**, le modifiche apportate dall'art. 15 al d. lgs. n. 65/2018:

D.Lgs. 65/2018	
TESTO PREVIGENTE	TESTO MODIFICATO DALL'ART. 15 DEL D.L. 82/2021, COME MODIFICATO IN SEDE REFERENTE
Art. 1	Art. 1
omissis	*omissis*
2. Ai fini del comma 1, il presente decreto prevede:	2. Ai fini del comma 1, il presente decreto prevede:
a) l'inclusione nella strategia nazionale di sicurezza cibernetica di previsioni in materia di sicurezza delle reti e dei sistemi informativi rientranti nell'ambito di applicazione del presente decreto;	a) l'inclusione nella **strategia nazionale di cybersicurezza** di previsioni in materia di sicurezza delle reti e dei sistemi informativi rientranti nell'ambito di applicazione del presente decreto;
b) la designazione delle autorità nazionali competenti e del punto di contatto unico, nonché del Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) in ambito nazionale per lo svolgimento dei compiti di cui all'allegato I;	b) la designazione dell'**autorità nazionale competente NIS, delle autorità di settore** e del punto di contatto unico, nonché del Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) in ambito nazionale per lo svolgimento dei compiti di cui all'allegato I;
omissis	*omissis*
Art. 3	Art. 3
1. Ai fini del presente decreto si intende per:	1. Ai fini del presente decreto si intende per:
a) autorità competente NIS, l'autorità competente per settore, in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1;	a) autorità **nazionale** competente NIS**, l'autorità nazionale unica,** competente in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1;
	***a*-bis*)* autorità di settore, le autorità di cui all'articolo 7, comma 1, lettere da *a)* a *e)*;**
omissis	*omissis*
Art. 4	Art. 4
omissis 6. L'elenco degli operatori di servizi essenziali identificati ai sensi del	*omissis* 6. L'elenco degli operatori di servizi essenziali identificati ai sensi del

comma 1 è riesaminato ~~con le medesime modalità di cui al comma 1~~ e, se del caso, aggiornato su base regolare, ed almeno ogni due anni dopo il 9 maggio 2018, ~~a cura delle autorità competenti NIS ed è comunicato al Ministero dello sviluppo economico.~~	comma 1 è riesaminato e, se del caso, aggiornato su base regolare, e almeno ogni due anni dopo il 9 maggio 2018, con le seguenti modalità:
	a) le autorità di settore, in relazione ai settori di competenza, propongono all'autorità nazionale competente NIS le variazioni all'elenco degli operatori dei servizi essenziali, secondo i criteri di cui ai commi 2 e 3;
	b) le proposte sono valutate ed eventualmente integrate, d'intesa con le autorità di settore, dall'autorità nazionale competente NIS che, con propri provvedimenti, provvede alle variazioni dell'elenco degli operatori dei servizi essenziali, dandone comunicazione, in relazione ai settori di competenza, anche alle autorità di settore.
omissis	*omissis*
Art. 5	Art. 5
1. Ai fini della determinazione della rilevanza degli effetti negativi di cui all'articolo 4, comma 2, lettera c), le autorità competenti NIS considerano i seguenti fattori intersettoriali:	1. Ai fini della determinazione della rilevanza degli effetti negativi di cui all'articolo 4, comma 2, lettera c), **l'autorità nazionale competente NIS e le autorità di settore** considerano i seguenti fattori intersettoriali:
omissis	*omissis*
Art. 6 Strategia nazionale di sicurezza cibernetica	Art. 6 Strategia nazionale di **cybersicurezza**
1. Il Presidente del Consiglio dei ministri adotta, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), la strategia nazionale di sicurezza cibernetica per	1. Il Presidente del Consiglio dei ministri adotta, sentito il **Comitato interministeriale per la cybersicurezza (CIC),** la strategia nazionale di **cybersicurezza** per la

la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. 2. Nell'ambito della strategia nazionale di sicurezza cibernetica, sono in particolare indicati, per la sicurezza di reti e sistemi informativi rientranti nell'ambito di applicazione del presente decreto:	tutela della sicurezza delle reti e dei sistemi di interesse nazionale. 2. 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;	*Identica*
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;	*Identica*
c) le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato;	*Identica*
d) i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi;	*Identica*
e) i piani di ricerca e sviluppo;	*Identica*
f) un piano di valutazione dei rischi;	*Identica*
g) l'elenco dei vari attori coinvolti nell'attuazione.	*Identica*
3. Con la procedura di cui al comma 1 sono adottate linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica.	3. Con la procedura di cui al comma 1 sono adottate linee di indirizzo per l'attuazione della strategia nazionale di **cybersicurezza**.
4. La Presidenza del Consiglio dei ministri trasmette la strategia nazionale in materia di sicurezza cibernetica alla Commissione europea entro tre mesi dalla sua adozione. Può essere esclusa la trasmissione di elementi della strategia riguardanti la sicurezza nazionale.	4. **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.
Art. 7	Art. 7

Autorità nazionali competenti e punto di contatto unico	**Autorità nazionale competente** e punto di contatto unico
1. Sono designate quali Autorità competenti NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III:	1. **L'Agenzia per la cybersicurezza nazionale è designata quale autorità nazionale competente NIS** per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III. **Sono designate quali autorità di settore:**
a) il Ministero dello sviluppo economico ~~per il settore energia, sottosettori energia elettrica, gas e petrolio e~~ per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali;	a) il Ministero dello sviluppo economico, per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali;
b) il Ministero delle infrastrutture e dei trasporti per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;	b) il Ministero delle infrastrutture **e della mobilità sostenibili,** per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;
c) il Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob, secondo modalità di collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze;	*Identica*
d) il Ministero della salute, per l'attività di assistenza sanitaria, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le	*Identica*

attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;	
	e) il Ministero della transizione ecologica per il settore energia, sottosettori energia elettrica, gas e petrolio;
e) il Ministero dell'ambiente e della tutela del territorio e del mare e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.	**f) il Ministero della transizione ecologica** e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.
2. Le Autorità competenti NIS sono responsabili dell'attuazione del presente decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e vigilano sull'applicazione del presente decreto a livello nazionale esercitando altresì le relative potestà ispettive e sanzionatorie.	2. **L'autorità nazionale competente NIS è responsabile** dell'attuazione del presente decreto con riguardo ai settori di cui all'allegato II e ai servizi di cui all'allegato III e **vigila** sull'applicazione del presente decreto a livello nazionale, esercitando altresì le relative potestà ispettive e sanzionatorie.
3. Il Dipartimento delle informazioni per la sicurezza (DIS) è designato quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi.	3. **L'Agenzia per la cybersicurezza nazionale** è designata quale punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi.
4. Il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità competenti NIS con le autorità competenti degli altri Stati membri, nonché con il gruppo di cooperazione di cui all'articolo 10 e la rete di CSIRT di cui all'articolo 11.	4. Il punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera **dell'autorità nazionale competente NIS** con le autorità competenti degli altri Stati membri, nonché con il gruppo di cooperazione di cui all'articolo 10 e la rete di CSIRT di cui all'articolo 11.
5. Il punto di contatto unico collabora nel gruppo di cooperazione in modo	*Identico*

effettivo, efficiente e sicuro con i rappresentanti designati dagli altri Stati.	
6. Le autorità competenti NIS e il punto di contatto unico consultano, conformemente alla normativa vigente, l'autorità di contrasto ed il Garante per la protezione dei dati personali e collaborano con essi.	6. **L'Agenzia per la cybersicurezza nazionale, in qualità di autorità nazionale competente NIS e di punto di contatto unico consulta**, conformemente alla normativa vigente, l'autorità di contrasto ed il Garante per la protezione dei dati personali e collaborano con essi.
7. La Presidenza del Consiglio dei ministri comunica tempestivamente alla Commissione europea la designazione del punto di contatto unico e quella delle autorità competenti NIS, i relativi compiti e qualsiasi ulteriore modifica. Alle designazioni sono assicurate idonee forme di pubblicità.	7. La Presidenza del Consiglio dei ministri comunica tempestivamente alla Commissione europea la designazione del punto di contatto unico e quella **dell'autorità nazionale competente NIS**, i relativi compiti e qualsiasi ulteriore modifica. Alle designazioni sono assicurate idonee forme di pubblicità.
8. Agli oneri derivanti dal presente articolo pari a 1.300.000 euro a decorrere dal 2018, si provvede ai sensi dell'articolo 22.	*Identico*
Art. 8	Art. 8
1. È istituito, presso la Presidenza del Consiglio dei ministri - Dipartimento delle informazioni per la sicurezza, il CSIRT italiano, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale, di cui all'articolo 16-bis del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82.	1. È istituito, presso **l'Agenzia di cybersicurezza nazionale**, il CSIRT italiano, che svolge i compiti e le funzioni del Computer Emergency Response Team (CERT) nazionale, di cui all'articolo 16-bis del decreto legislativo 1° agosto 2003, n. 259, e del CERT-PA, già operante presso l'Agenzia per l'Italia digitale ai sensi dell'articolo 51 del decreto legislativo 7 marzo 2005, n. 82.
omissis	*omissis*
Art. 9	Art. 9
1. Le autorità competenti NIS, il punto di contatto unico e il CSIRT italiano collaborano per	1. **Le autorità di settore** collaborano **con l'autorità nazionale competente NIS** per l'adempimento degli obblighi

l'adempimento degli obblighi di cui al presente decreto. A tal fine è istituito, presso la Presidenza del Consiglio dei ministri, un Comitato tecnico di raccordo, composto da rappresentanti delle amministrazioni statali competenti ai sensi dell'articolo 7, comma 1, e da rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati dalle Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. L'organizzazione del Comitato è definita con decreto del Presidente del Consiglio dei ministri, da adottare su proposta dei Ministri per la semplificazione e la pubblica amministrazione e dello sviluppo economico, sentita la Conferenza unificata. Per la partecipazione al Comitato tecnico di raccordo non sono previsti gettoni di presenza, compensi o rimborsi spese.	di cui al presente decreto. A tal fine è istituito presso **l'Agenzia per la cybersicurezza nazionale,** un Comitato tecnico di raccordo. **Il Comitato è presieduto dall'autorità nazionale competente NIS ed è** composto dai rappresentanti delle amministrazioni statali **individuate quali autorità di settore** e da rappresentanti delle Regioni e Province autonome in numero non superiore a due, designati dalle Regioni e Province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. L'organizzazione del Comitato è definita con decreto del Presidente del Consiglio dei ministri, sentita la Conferenza unificata. Per la partecipazione al Comitato tecnico di raccordo non sono previsti gettoni di presenza, compensi o rimborsi spese.
omissis	*omissis*
Art. 12	Art. 12
omissis	*omissis*
5. Gli operatori di servizi essenziali notificano al CSIRT italiano e, ~~per conoscenza, all'autorità competente NIS~~, senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.	5. Gli operatori di servizi essenziali notificano al CSIRT italiano senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali forniti.
6. Il CSIRT italiano inoltra tempestivamente le notifiche all'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato, ai sensi delle direttive del Presidente del Consiglio dei ministri adottate sentito il	6. Il CSIRT italiano inoltra tempestivamente le notifiche all'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato, ai sensi delle direttive del Presidente del Consiglio dei ministri adottate sentito il

Comitato interministeriale per la sicurezza della Repubblica (CISR), delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento.	**Comitato interministeriale per la cybersicurezza (CIC)**, delle attività di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento.
omissis	*omissis*
Art. 14	Art. 14
omissis	*omissis*
4. I fornitori di servizi digitali notificano al CSIRT italiano ~~e, per conoscenza, all'autorità competente NIS,~~ senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla fornitura di un servizio di cui all'allegato III che essi offrono all'interno dell'Unione europea.	4. I fornitori di servizi digitali notificano al CSIRT italiano senza ingiustificato ritardo, gli incidenti aventi un impatto rilevante sulla fornitura di un servizio di cui all'allegato III che essi offrono all'interno dell'Unione europea.
omissis	*omissis*
Art. 19	Art. 19
1. L'attività di ispezione e verifica necessarie per le misure previste dagli articoli 12, 13, 14 e 15, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica, sono svolte dalle autorità competenti NIS.	1. L'attività di ispezione e verifica necessarie per le misure previste dagli articoli 12, 13, 14 e 15, fatte salve le attribuzioni e le competenze degli organi preposti alla tutela dell'ordine e della sicurezza pubblica, sono svolte **dall'autorità nazionale competente NIS**.
2. Con successivo Accordo tra Governo, Regioni e Province autonome di Trento e di Bolzano sono definiti i criteri uniformi in ambito nazionale per lo svolgimento delle attività di ispezione e verifica, necessarie per le misure previste dagli articoli 12, 13, 14 e 15, che riguardano le reti e i sistemi informativi utilizzati dagli operatori che prestano attività di assistenza sanitaria, nonché in merito al settore fornitura e distribuzione di acqua potabile.	***Soppresso.***

Art. 20	Art. 20
1. Le autorità competenti NIS di cui all'articolo 7, comma 1, lettere a), b), c), d) ed e), per i rispettivi settori e sottosettori di riferimento di cui all'allegato II e per i servizi di cui all'allegato III, sono competenti per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative previste dal presente decreto.	1. **L'autorità nazionale competente NIS è competente** per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative previste dal presente decreto.
omissis	*omissis*
Allegato I	Allegato I
omissis	*omissis*
I requisiti e i compiti del CSIRT sono adeguatamente e chiaramente definiti ai sensi del presente decreto e del decreto del Presidente del Consiglio dei ministri di cui all'art. 8, comma 2. Essi includono quanto segue: 1. Requisiti per il CSIRT a) Il CSIRT garantisce un alto livello di disponibilità dei propri servizi di comunicazione, evitando singoli punti di guasto, e dispone di vari mezzi che permettono allo stesso di essere contattato e di contattare altri in qualsiasi momento. Inoltre, i canali di comunicazione sono chiaramente specificati e ben noti alla loro base di utenti e ai partner con cui collaborano. b) I locali del CSIRT e i sistemi informativi di supporto sono ubicati in siti sicuri. c) Continuità operativa: i. il CSIRT è dotato di un sistema adeguato di gestione e inoltro delle richieste in modo da facilitare i passaggi;	*Identico*

ii. il CSIRT dispone di personale sufficiente per garantirne l'operatività 24 ore su 24; iii. il CSIRT opera in base a un'infrastruttura di cui è garantita la continuità. A tal fine è necessario che siano disponibili sistemi ridondanti e spazi di lavoro di backup. d) il CSIRT ha la possibilità, se lo desidera, di partecipare a reti di cooperazione internazionale.	
	d-bis) **il CSIRT Italia conforma i propri servizi e la propria attività alle migliori pratiche internazionalmente riconosciute in materia di prevenzione, gestione e risposta rispetto a eventi di natura cibernetica.**
(…)	(…)
2. Compiti del CSIRT a) I compiti del CSIRT comprendono almeno: i. monitoraggio degli incidenti a livello nazionale; ii. emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; iii. intervento in caso di incidente; iv. analisi dinamica dei rischi e degli incidenti, nonché sensibilizzazione situazionale; v. partecipazione alla rete dei CSIRT b) il CSIRT stabilisce relazioni di cooperazione con il settore privato;	*Identica*
c) per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate nei seguenti settori:	c) per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate**, secondo le migliori pratiche internazionalmente riconosciute,** nei seguenti settori:

i. procedure di trattamento degli incidenti e dei rischi; ii. sistemi di classificazione degli incidenti, dei rischi e delle informazioni.	i. procedure di trattamento degli incidenti e dei rischi; ii. sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

Articolo 16, commi 1-7
(Modifiche alla legge n. 124 del 2007 e al decreto-legge n. 105/2019)

L'**articolo 16** reca alcune modifiche puntuali alla legislazione vigente conseguenti al nuovo assetto dell'architettura nazionale di cybersicurezza disposta dal decreto in esame. Si tratta principalmente delle modifiche che consentono il passaggio delle competenze in materia di perimetro di sicurezza nazionale dal DIS e dal MISE all'Agenzia per la cybersicurezza nazionale nonché quelle relative, in particolare, al Centro di Valutazione e Certificazione Nazionale (CVCN) e quelle di competenza dell'AgID.

A tal fine l'articolo 16 interviene sulla disciplina recata dal decreto-legge n. 105 del 2019 che ha, in particolare, istituito il perimetro di sicurezza cibernetica e dalla legge n. 124 del 2007, che reca la disciplina del Sistema di informazione per la sicurezza della Repubblica, per le parti in cui sono previste diverse attribuzioni di competenza.

Il **comma 1** modifica l'articolo 3, comma 1-*bis* della legge 124/2007 che, nel testo previgente, non consente all'Autorità delegata di esercitare **funzioni** di governo **ulteriori** rispetto a quelle ad essa delegate dal Presidente del Consiglio dei ministri nell'ambito del sistema di informazioni per la sicurezza della Repubblica a norma della medesima legge 124. Con il comma in esame si consente all'Autorità delegata di svolgere anche le funzioni "in materia di cybersicurezza".

La modifica è posta in relazione con l'articolo 3 del decreto in esame che dà facoltà al Presidente del Consiglio di delegare le competenze in materia di cibersicurezza alla medesima Autorità delegata per la sicurezza della Repubblica, se istituita.

> Si ricorda che, in base alla legge n. 124 del 2007, il **Sistema di informazione per la sicurezza** della Repubblica è composto dal Presidente del Consiglio dei ministri, dal Comitato interministeriale per la sicurezza della Repubblica (CISR), dall'**Autorità eventualmente delegata dal Presidente del Consiglio**, dal Dipartimento delle informazioni per la sicurezza (DIS), e dai servizi di informazione: Agenzia informazioni e sicurezza esterna (AISE) e Agenzia informazioni e sicurezza interna (AISI).

Il **comma 2** abroga il comma 1-*bis* dell'articolo 38 della legge 124/2007, a decorrere **dal 1° gennaio 2023**, come specificato nel corso dell'**esame in sede referente**. Tale disposizione prevede che alla relazione

annuale sulla **politica dell'informazione** per la sicurezza e sui risultati ottenuti (da trasmettere al Parlamento entro il mese di febbraio), sia allegato il **documento di sicurezza nazionale**, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica.

La modifica è conseguente con quanto previsto dall'articolo 14 del presente provvedimento che dispone in ordine alla trasmissione al Parlamento delle relazioni annuali in materia di cibersicurezza (v. *supra*).

A decorrere dal 1° gennaio 2023, pertanto, alla relazione annuale sulla politica dell'informazione per la sicurezza e sui risultati ottenuti non deve essere più allegato il documento di sicurezza nazionale concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla **protezione cibernetica** e alla sicurezza informatica.

Ai sensi del **comma 3** la denominazione **CSIRT Italia** (*Computer Security Incident Response Team*) sostituisce, ovunque presente, quella di CSIRT Italiano.

Seguono una serie di modifiche alla legislazione vigente dovute al trasferimento di competenze operate dal provvedimento in esame.

In particolare nel decreto-legge 105/2019 (perimetro cibernetico):

- le parole: «Comitato interministeriale per la sicurezza della Repubblica (CISR)» e «CISR», ovunque ricorrano, sono rispettivamente sostituite dalle seguenti: «Comitato interministeriale per la cybersicurezza (CIC)» e «CIC», ad eccezione per le disposizioni di cui all'articolo 5 del medesimo decreto-legge (**comma 4**);

L'articolo 1, comma 7 del DL 105/2019 affida all'organismo tecnico di supporto al CISR il compito di rendere avviso sugli schemi di certificazione cibernetica elaborato dal CVCN. A seguito della modifica apportata dal comma 4 il riferimento è "all'organismo tecnico di supporto al CIC". Andrebbe pertanto valutata l'opportunità di chiarire gli elementi a quale organismo si riferisca la disposizione.

- i riferimenti al Dipartimento delle informazioni per la sicurezza, o al DIS, ovunque ricorra, sono da intendersi riferiti all'Agenzia per la cybersicurezza nazionale e i riferimenti al Nucleo per la sicurezza cibernetica sono da intendersi riferito al Nucleo per la cybersicurezza, salvo, secondo quanto previsto da una disposizione introdotta in **sede**

referente, che nelle disposizioni di cui all'articolo 1, comma 2, lettera *b)*, e all'articolo 1, comma 2-*ter*, del medesimo decreto-legge (su cui interviene il comma 9 lett. a-*ter)* e a-*quater)* del presente articolo -v. *infra*) relative all'elenco delle reti, dei sistemi informativi e dei servizi informatici rientranti nel perimetro della sicurezza cibernetica (**comma 5**).

- i riferimenti al Ministero dello sviluppo economico e alla Presidenza del Consiglio dei ministri, ovunque ricorrano, sono da intendersi riferito all'Agenzia per la cybersicurezza nazionale (**comma 6, lettera *a***);
- le eventuali misure di sicurezza aggiuntive che devono osservare gli operatori dei servizi essenziali, i fornitori dei servizi digitali e le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico sono definite dalla Agenzia per la cybersicurezza nazionale, in luogo della Presidenza del Consiglio (per i soggetti pubblici) e del MISE (per i soggetti privati) (**comma 6, lettera *b*)**;
- si specifica che il CSIRT Italia inoltra le notifiche sugli eventuali incidenti che coinvolgono reti, sistemi informativi e servizi informatici all'autorità competente nazionale NIS di cui all'articolo 7 del D.Lgs. 65/2018 (**comma 6, lettera *c*)**.

Ai sensi del **comma 7** nei provvedimenti attuativi di natura regolamentare e amministrativa previsti dall'articolo 1 del medesimo DL 105/2019 i riferimenti al CISR e al DIS sono da intendersi al CIC e all'Agenzia per la cybersicurezza nazionale (per l'illustrazione di tali provvedimenti si veda il paragrafo sul *Quadro normativo*).

Articolo 16, commi 8-14
(Altre modificazioni)

L'**articolo 16, commi 8-14,** modificato nel corso dell'esame in sede referente, reca innanzi tutto alcune disposizioni di modifica del decreto-legge n. 105 del 2019 volte ad adeguare le disposizioni del citato decreto-legge alle modifiche intervenute e a rendere più fluide, a seguito di modifiche introdotte in sede referente, le comunicazioni tra i vari soggetti responsabili per la cybersicurezza (**commi 8 e 9**), il **comma 10** modifica, al fine di integrare con il riferimento ai test effettuati dal CVCN, le disposizioni del decreto-legge n. 21 del 2012 in merito alle comunicazioni da effettuare a cura delle imprese acquirenti impianti per il 5G ai fini dell'esercizio dei poteri speciali, prevedendo inoltre alcune integrazioni e alcune semplificazioni procedurali, il **comma 11** inserisce tra le ipotesi di competenza del TAR del Lazio, sede di Roma, le controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale nonchè, come specificato in sede referente, quelle sul rapporto di lavoro del personale dell'Agenzia; i **commi 12, 13 e 14** aggiornano al nuovo quadro normativo, con particolare riferimento alle funzioni della citata dell'Agenzia per la cybersicurezza nazionale, le disposizioni della legge di delegazione europea 2019-2020 (comma 12), quelle relative alla definizione della competenza regolamentare in materia di sicurezza e qualità delle infrastrutture digitali per la pubblica amministrazione (comma 13) e del Codice delle Comunicazioni elettroniche (comma 14).

In particolare il **comma 8** adegua le disposizioni del decreto-legge 21 settembre 2019, n. 105 (decreto-legge perimetro), con riferimento al contenuto dei provvedimenti di natura regolamentare e amministrativa la cui adozione è prevista dall'articolo l del citato decreto-legge. Si prevede in particolare che i riferimenti contenuti nei citati atti attuativi al Ministero dello sviluppo economico e alla struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e la digitalizzazione - fatta eccezione per le disposizioni di cui agli articoli 3 del decreto del Presidente del Consiglio dei ministri n. 131 del 2020 - vadano riferiti all'Agenzia per la cybersicurezza nazionale istituita ai sensi dell'articolo 5 del decreto in esame.

L'articolo 3 del decreto del Presidente del Consiglio dei ministri n. 131 del 2020 indica le istituzioni tenute all'individuazione dei soggetti da includere nel perimetro di sicurezza nazionale indicando che il per il settore servizi digitali, sia il Ministero dello sviluppo economico, in raccordo con la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica

e la digitalizzazione, per il settore tecnologie critiche, la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, in raccordo con il Ministero dello sviluppo economico e con il Ministero dell'università e della ricerca e per il settore energia, il Ministero dello sviluppo economico. Tali competenze restano affidate ai soggetti sopra indicati.

Il **comma 9** reca alcune modifiche a decreto-legge 21 settembre 2019, n. 105 (decreto-legge perimetro).

In particolare, la **lettera a)** prevede che l'obbligo di comunicazione al CVCN del Ministero dello sviluppo economico dell'intendimento di acquisire beni, sistemi e servizi ICT da impiegare sulle reti sensibili dei soggetti rientranti nel perimetro di sicurezza nazionale sia efficace a decorrere dal trentesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale del decreto del Presidente del Consiglio dei Ministri che - sentita l'Agenzia per la cybersicurezza nazionale - attesta l'operatività del CVCN e comunque dal 30 giugno 2022.

L'**articolo 6, comma 1, lettera a), del decreto-legge n. 105 del 2019** prevede, nell'ambito del regolamento previsto dal comma 6 dell'articolo 1, che disciplina diversi profili concernenti le attività dei soggetti rientranti nel perimetro di sicurezza nazionale, con riferimento all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, appartenenti a categorie individuate sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, che tali soggetti diano comunicazione di tale intendimento al Centro di valutazione e certificazione nazionale (CVCN), istituito da tale decreto-legge presso il Ministero dello sviluppo economico (e ora trasferito all'Agenzia).

Nel corso dell'esame in sede referente **è stata introdotta la lettera a-*bis*)** che ha modificato **l'articolo 1, comma 7, lettera c)** al fine di sostituire il riferimento all'organismo tecnico di supporto al CISR con quello al Tavolo interministeriale di cui all'articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131 **nonché le lettere a-*ter*)** e **a-*quater*).**

La lettera **a-*bis)* sostituisce la lettera b) del comma 2 dell'articolo 1 del decreto-legge,** tuttavia rispetto al testo vigente sono introdotte esclusivamente le seguenti modifiche:

- l'individuazione dei **criteri** con i quali i soggetti di cui al comma 2-bis predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici rientranti nel perimetro della sicurezza cibernetica viene affidata al **Tavolo interministeriale** per l'attuazione del perimetro di sicurezza nazionale cibernetica (previsto dall'articolo 6 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131) anziché dall' organismo tecnico di supporto al CIC.

Si ricorda che il Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica è presieduto da un vicedirettore generale del DIS, ed è composto da due rappresentanti di ciascuna amministrazione CISR, da un rappresentante per ciascuna delle due Agenzie, nonché da due rappresentanti degli altri Ministeri di volta in volta interessati, che sono chiamati a partecipare alle riunioni, anche su loro richiesta motivata, in relazione agli argomenti da trattare, di cui almeno uno in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica.

- gli elenchi dei sistemi informativi e dei servizi informatici rientranti nel perimetro della sicurezza cibernetica sono inviati all'Agenzia per la cybersicurezza nazionale, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza anziché alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico;
- il Dipartimento delle informazioni per la sicurezza, l'AISE e l'AISI (ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7, della legge n. 124 del 2007), nonché l'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144 **accedono direttamente a tali elenchi** per il tramite della piattaforma digitale costituita presso l'Agenzia per la cybersicurezza nazionale **invece di ricevere l'elenco di tali sistemi** a cura di Presidenza del Consiglio dei ministri e Ministero dello sviluppo economico.

La lettera **a-*ter)*** prevede poi che gli elenchi dei soggetti rientranti nel perimetro di sicurezza nazionale siano trasmessi al Dipartimento delle informazioni per la sicurezza, che provvede anche a favore dell'AISE e

dell'AISI ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7, della legge n. 124 del 2007.

In base a queste disposizioni rientrano tra tali funzioni: il rafforzamento delle attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali (art. 1, comma 3-*bis*), il coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali nonché gli altri compiti del DIS (art. 4) e le attività istituzionali facenti capo all'AISE (art. 6) e all'AISI (art. 7).

La **lettera b)** abroga il comma 2 dell'articolo 3 del decreto legge n. 105 del 2019.

L'**articolo 3, comma 2 del decreto legge n. 105 del 2019** prevedeva che dalla data di entrata in vigore del regolamento previsto dall'articolo 1, comma 6, i poteri speciali di cui all'articolo 1-bis del decreto-legge 15 marzo 2012, n. 21 sono esercitati previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, da parte dei centri di valutazione e certificazione nazionale (CVCN) previsti all'articolo 1, comma 6, lettera a).

La **lettera c) n. 1,** prevede che, a decorrere dalla data in cui diviene efficace l'obbligo di comunicazione disciplinato dalla lettera a) del comma in commento, i soggetti che intendono procedere all'acquisizione. a qualsiasi titolo di beni, servizi e componenti per le reti 5G (di cui all'articolo 1-bis, comma 2 del decreto-legge n. 21 del 2012) sono obbligati ad effettuare la comunicazione di cui all'articolo l, comma 6, lettera a), per lo svolgimento delle verifiche di sicurezza da parte del CVCN sulla base delle procedure, delle modalità e dei termini previsti dal regolamento di attuazione. Ai fornitori dei predetti beni, servizi e componenti si applica l'articolo l, comma 6, lettera b).

L'**articolo 1-bis, comma 2 del decreto-legge n. 21 del 2012** prevede che la stipula di contratti o accordi aventi ad oggetto l'acquisizione, a qualsiasi titolo, di beni o servizi o componenti ad alta intensità tecnologica relativi alle reti 5G è soggetta alla notifica al fine dell'eventuale esercizio del potere di veto o dell'imposizione di specifiche prescrizioni o condizioni.

L'articolo 1, comma 6, lettera b) prevede che i fornitori di beni servizi e sistemi devono fornire la propria collaborazione al CVCN e, limitatamente agli ambiti di specifica competenza, ai Centri di valutazione operanti presso i Ministeri dell'interno e della difesa per l'effettuazione delle attività di test, sostenendone gli oneri.

La **lettera c), n. 2**, abroga il comma 3 dell'articolo 3 del decreto-legge n. 105 del 2019.

Tale disposizione prevedeva che entro sessanta giorni dalla data di entrata in vigore del regolamento di cui all'articolo 1, comma 6, le condizioni e le prescrizioni relative ai beni e servizi concernenti le reti 5G acquistati con contratti già autorizzati con decreti del Presidente del Consiglio dei ministri, in data anteriore alla data di entrata in vigore del medesimo regolamento, se attinenti alle reti, ai sistemi informativi e ai servizi informatici critici, potevano essere modificate o integrate, se, a seguito della valutazione svolta da parte dei centri di valutazione di cui all'articolo fossero emersi elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, con misure aggiuntive necessarie al fine di assicurare livelli di sicurezza equivalenti a quelli previsti dal decreto-legge n. 105 del 2019, anche prescrivendo la sostituzione di apparati o prodotti, ove indispensabile al fine di risolvere le vulnerabilità accertate.

Le modifiche del comma 9, insieme con quelle dei commi 8 e 10, secondo quanto indicato nella relazione illustrativa, sono finalizzate ad assicurare le disposizioni che disciplinano il Centro di valutazione e certificazione nazionale siano efficaci al momento della piena operatività del Centro.

Si ricorda che, ai sensi dell'articolo 7 comma 4 del decreto in esame "Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia nazionale per la cybersicurezza" e che, ai sensi dell'articolo 7, comma 1, lettera *f)*, n. 1, sono trasferite alla medesima agenzia le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, nonché quelle relative "al perimetro di sicurezza nazionale cibernetica" ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto-legge perimetro. Alla luce di quanto previsto dal comma in commento rimangono in capo al Centro di valutazione e certificazione nazionale le comunicazioni concernenti l'intendimento di acquisizione di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti sensibili rientranti nel perimetro della sicurezza nazionale, a condizione che sia attestata l'operatività del CVCN medesimo (comunque trasferito all'Agenzia). Sembrerebbe quindi che, allo stato, il CVCN non risulti operativo. Risulterebbero inoltre in capo al CVCN le altre funzioni di cui all'articolo 1, comma 6, lettera a) per le quali non sono previste modificazioni.

Si valuti l'opportunità di chiarire maggiormente le previsioni del comma 9 alla luce del trasferimento del CVCN presso l'Agenzia ai sensi dell'art. 7.

Il **comma 10** disciplina le modalità di comunicazione dei contratti o degli accordi concernenti l'acquisizione di beni, reti o servizi funzionali al 5G, a questo scopo novellando il comma 3-bis dell'articolo 1-bis del decreto-legge n. 21 del 2012. Pur prevedendosi una novella integrale del testo del comma 3-*bis*, in realtà, il testo appare in larga parte coincidente con la disciplina precedentemente vigente.

Rispetto a quanto previsto dalla disciplina precedentemente vigente sono introdotte esclusivamente le seguenti modifiche:

- si prescrive che nell'informativa che l'impresa acquirente deve fornire alla Presidenza del Consiglio dei ministri funzionale alla decisione di esercitare i poteri speciali debba essere fornita **anche la comunicazione del Centro di valutazione e certificazione nazionale (CVCN),** relativa all'esito della valutazione da esso effettuata e alle eventuali prescrizioni;

- si prevede conseguentemente che, qualora il contratto sia stato stipulato antecedentemente alla conclusione dei test imposti dal CVCN, il termine **di 10 giorni** per l'invio dell'informativa **decorre** dalla comunicazione di esito positivo della valutazione effettuata dal CVCN;

- viene soppresso il periodo che prevedeva che qualora sia necessario svolgere approfondimenti riguardanti aspetti tecnici relativi alla valutazione di possibili fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano, il termine di trenta giorni per la conclusione del procedimento per l'esercizio dei poteri speciali potesse essere prorogato fino a venti giorni, prorogabili ulteriormente di venti giorni, per una sola volta, in casi di particolare complessità;

- viene introdotta, tra le fattispecie che giustificano l'irrogazione di sanzioni amministrative il caso in cui l'impresa abbia eseguito il contratto o l'accordo in violazione del decreto di esercizio dei poteri speciali;

- sono previste **alcune riformulazioni di carattere formale** (viene soppresso il riferimento all'undicesimo periodo del comma 3-bis con riferimento alla disciplina delle sanzioni, viene soppresso l'inciso "nel provvedimento di esercizio dei predetti poteri" nella disposizione che consente al Governo di ordinare all'impresa di ripristinare la situazione anteriore e viene altresì soppressa, nel medesimo periodo dopo la parola anteriore, l'espressione "all'esecuzione del predetto contratto o accordo").

Il **comma 11** inserisce, mediante novella al Codice del processo amministrativo (art. 135, D.Lgs. n. 104 del 2010) tra le ipotesi di competenza funzionale inderogabile del **Tribunale amministrativo regionale del Lazio, sede di Roma,** anche le controversie aventi ad oggetto i **provvedimenti** dell'Agenzia per la cybersicurezza nazionale.

Nel corso dell'esame in sede referente è stata inoltre modificata la lettera o) del medesimo articolo 135 del decreto legislativo n. 104 del 2010 al fine di inserire tra le fattispecie di competenza funzionale inderogabile del TAR del Lazio, sede di Roma, anche le controversie relative al **rapporto di lavoro** del personale dell'Agenzia per la cybersicurezza nazionale.

Il **comma 12** modifica l'articolo 4, comma 1, lettera b), della legge di delegazione europea 2019-2020, che indica i principi ed i criteri direttivi relativi per il recepimento del nuovo codice europeo delle comunicazioni elettroniche, al fine di inserire il riferimento alla nuova Agenzia per la cybersicurezza nazionale tra le autorità competenti per l'attuazione delle disposizioni del Codice stesso e l'articolo 18 della legge di delegazione europea 2019-2020, contenente i principi e criteri direttivi per l'adeguamento della normativa nazionale al Regolamento europeo sulla cybersicurezza (Regolamento (UE) 2019/881) al fine di prevedere che ogni riferimento al Ministero dello sviluppo economico, sia da intendersi riferito all'Agenzia per la cybersicurezza nazionale.

Il **comma 13** aggiorna, alla luce dell'istituzione dell'Agenzia per la cybersicurezza nazionale e delle funzioni ad essa attribuite, il riferimento contenuto all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, al fine di attribuire all'Agenzia - e non più all'Agid - il potere regolamentare di disciplinare la definizione dei livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione nonché le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi *cloud* per la pubblica amministrazione oltre che la migrazione dei CED delle pubbliche amministrazioni e degli enti locali. A seguito di una modifica introdotta in sede referente è stato inoltre attribuita all'Agenzia la definizione delle modalità del procedimento di qualificazione dei servizi *cloud* per la pubblica amministrazione.

Il **comma 14** modifica (comma 14, lett. a), al fine di adeguare al nuovo quadro normativo derivante dal decreto-legge in commento, gli articoli 16-*bis* e 16-*ter* del Codice delle comunicazioni elettroniche (decreto legislativo n. 259 del 2003), attribuendo all'Agenzia per la cybersicurezza nazionale le funzioni, precedentemente in capo al Ministero dello sviluppo

economico, in materia di individuazione delle misure di natura tecnica e organizzativa per assicurare la sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico, nonché per garantire l'integrità delle citate reti e dei casi in cui le violazioni della sicurezza o perdita dell'integrità siano da considerarsi significative ai fini del corretto funzionamento delle reti o dei servizi (articolo 16-*bis*) nonché i poteri di verifica della sicurezza, di indagine sui casi di mancata conformità nonché sui loro effetti sulla sicurezza e l'integrità delle reti e di irrogazione delle sanzioni per il mancato rispetto delle citate disposizioni (art. 16-*ter*).

Con riferimento ai poteri di verifica della sicurezza è altresì soppressa la collaborazione con gli Ispettorati territoriali del Ministero dello sviluppo economico (comma 14, lett. c).

Si prevede infine (comma 14, lett. b) che le misure adottate ai fini dell'attuazione degli articoli 16-*bis* e 16-*ter* siano approvate con decreto del Presidente del Consiglio dei ministri (anziché del Ministro dello sviluppo economico).

Articolo 17
(Disposizioni transitorie e finali)

L'**articolo 17**, modificato in **sede referente,** reca disposizioni transitorie e finali.

Il **comma 1** prevede che per lo **svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni**, attribuite alla neo-istituita Agenzia per la cybersicurezza nazionale (cfr. articolo 7 *supra*), essa possa avvalersi "dell'ausilio" del **personale dell'organo centrale del Ministero dell'interno** per la sicurezza e la regolarità dei servizi delle telecomunicazioni (previsto dall'articolo 7-*bis* del decreto-legge n. 144 del 2005; ossia il Servizio di polizia postale e delle comunicazioni del Dipartimento della pubblica sicurezza).

Il **comma 2** dispone che la nascente Agenzia operi "con l'ausilio" dell'organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni, per quanto concerne le **funzioni di attuazione e di controllo** dell'esecuzione dei provvedimenti del Presidente del Consiglio indicati dall'articolo 5 del decreto-legge n. 105 del 2019 recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.

Ai sensi di quell'articolo 5 così richiamato, il Presidente del Consiglio dei ministri, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, può disporre, ove indispensabile e per il tempo strettamente necessario, secondo criteri di proporzionalità, la disattivazione, totale o parziale di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati.

Il **comma 3** stabilisce che il "personale dell'Agenzia", nello svolgimento delle funzioni richiamato nei commi 1 e 2 del medesimo articolo 17, rivesta la qualifica di **pubblico ufficiale** (*si valuti l'opportunità di specificare se in tale ambito si intenda ricomprendere anche il personale* dell'organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni, del quale l'Agenzia si avvale ai sensi dei commi 1 e 2).

Il **comma 4** concerne il personale dell'Agenzia addetto al CSIRT Italia (trasferito presso l'Agenzia dall'articolo 7 del presente decreto-legge, v.

scheda s*upra*). Anche questo personale, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale.

Lo CSIRT, acronimo che sta per *Computer Security Incident Response Team*, è – come ricordato - una struttura i cui compiti sono definiti dal decreto legislativo 18 maggio 2018, n. 65 ("Attuazione della direttiva UE 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione") e dal decreto del Presidente del Consiglio dei ministri 8 agosto 2019 ("Disposizioni sull'organizzazione e il funzionamento del *Computer security incident response team* - CSIRT italiano"). Tra questi, vi sono: il monitoraggio degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale.

La trasmissione delle notifiche di incidente, che rientra tra i compiti del CSIRT, è inquadrata tra gli obblighi di denuncia fissati dall'articolo 331 del codice di procedura penale, concernente appunto la **denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio - ancora prevede il comma 4 del presente articolo del decreto-legge.**

Il **comma 5** demanda ad **uno o più decreti del Presidente del Consiglio dei ministri** la definizione di termini e di modalità per assicurare la **prima operatività dell'Agenzia**, onde trasferire funzioni, beni strumentali e documentazione, attuare le disposizioni del decreto-legge, regolare le riduzioni di risorse finanziarie relative alle amministrazioni cedenti.

I D.P.C.M. sono da adottarsi **entro centottanta giorni** dall'entrata in vigore del decreto-legge.

Circa la prima operatività dell'Agenzia, saranno stabilite intese con le amministrazioni interessate ed individuati appositi spazi in via transitoria, nel rispetto delle specifiche norme riguardanti l'organizzazione e il funzionamento. *Si valuti in proposito l'opportunità di una maggiore specificazione del richiamo a tali norme.*

Con una disposizione inserita in sede referente (comma 5-*bis*) è stabilito che la gestione delle risorse finanziarie relative alle funzioni trasferite compete alle amministrazioni cedenti fino alla scadenza dei termini indicati nei dPCm per la prima operatività dell'Agenzia. A decorrere da tale data l'Agenzia assume la titolarità di tutti di rapporti giuridici attivi e passivi relativi alle funzioni trasferite.

Con D.P.C.M. è altresì definito - aggiunge il **comma 6** - il dovuto raccordo tra la neo-istituita Agenzia e l'Agenzia per l'Italia digitale (AgID), per quanto concerne il trasferimento di funzioni da questa a quella (previsto dall'articolo 7 del decreto-legge, v. *supra*).

In sede referente è stato inoltre previsto che nelle more dell'adozione dei dPCm di cui al comma 5, il regolamento sulle **infrastrutture digitali delle p.a.** (di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, conv. L. n. 221 del 2012), è adottato dall'**AgID**, d'intesa con la competente struttura della Presidenza del Consiglio dei ministri.

Si ricorda che in proposito che il regolamento di cui alla norma citata deve stabilire i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle **infrastrutture digitali per la pubblica amministrazione**. Definisce, inoltre, le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei **servizi cloud** per la pubblica amministrazione.

Il **comma 7** prevede che il direttore generale dell'Agenzia identifichi, assuma e liquidi gli impegni di spesa, che il Dipartimento delle informazioni per la sicurezza provvederà a pagare nell'ambito delle risorse destinate appunto all'Agenzia. A tal fine, come precisato in sede referente, è istituito un apposito capitolo nel bilancio del DIS. Questo, fino all'adozione di un regolamento di contabilità dell'Agenzia che ne assicuri l'autonomia gestionale e contabile, e di un regolamento sulle procedure per la stipula di contratti di appalti di lavori e forniture di beni (atti previsti dall'articolo 11 del decreto-legge).

Il **comma 8** concerne l'**inizio dell'operatività della nuova Agenzia** sotto il profilo delle dotazioni di **organico** e dei relativi oneri.

A seguito delle modifiche introdotte in sede referente, si prevede in primo luogo che dalla data della nomina del Direttore dell'Agenzia il **Dipartimento delle informazioni per la sicurezza (DIS)** metta a disposizione il **personale** impiegato nell'ambito delle attività relative allo svolgimento delle funzioni oggetto di trasferimento, con modalità da definire mediante **intese** con lo stesso Dipartimento (lett. a)).

Inoltre si stabilisce che per un periodo massimo di sei mesi - prorogabile una sola volta, per un massimo di ulteriori sei mesi – l'Agenzia si **avvalga di personale appartenente** al Ministero dello sviluppo economico, all'Agenzia per l'Italia digitale, **ad altre pubbliche amministrazioni** e ad autorità indipendenti, messo a disposizione dell'Agenzia stessa su specifica richiesta e secondo modalità individuate mediante intese con le rispettive amministrazioni di appartenenza (lett. b).

Numericamente, il personale esterno temporaneamente a disposizione dell'Agenzia **non può eccedere il 30 per cento** della dotazione organica complessiva iniziale dell'Agenzia stessa.

I relativi oneri sono a carico delle amministrazioni di appartenenza (**comma 8-bis**).

Il **comma 9** dispone che il regolamento disciplinante l'ordinamento e il reclutamento del personale addetto all'Agenzia (previsto dall'articolo 12 del decreto-legge, v. *supra*) preveda modalità selettive per **l'inquadramento - nella misura massima del 50 per cento** della dotazione organica complessiva - del personale di primo avvalimento (ai sensi del comma 8, lett. *b)*) o del personale assunto a **tempo determinato** (ai sensi dell'articolo 12, comma 2, lettera *b)*), ove già appartenente a pubbliche amministrazioni. In sede referente è stato previsto che il personale del DIS impiegato per la prima operatività dell'Agenzia nell'ambito delle funzioni trasferite (di cui al comma 8, lettera *a)*), è inquadrato, a decorrere dal 1° gennaio 2022, nel ruolo del personale dell'Agenzia (di cui all'articolo 12, comma 2, lettera *a)*) secondo le modalità definite dal regolamento del personale.

Siffatto inquadramento è nel contingente di personale addetto all'Agenzia (su cui v. *supra* l'articolo 12 del presente decreto-legge).

Le modalità selettive tengono conto delle mansioni svolte e degli incarichi ricoperti durante il periodo di servizio presso l'Agenzia, nonché delle competenze possedute e dei requisiti di professionalità ed esperienza richiesti per le specifiche posizioni.

Ove si tratti del personale di primo avvalimento (ai sensi del comma 8), gli inquadramenti conseguenti alle procedure selettive decorrono allo scadere dei sei mesi, o della relativa proroga, e comunque, non oltre il 30 giugno 2022.

Il **comma 10** inserisce la nascente Agenzia tra le articolazioni dell'Amministrazione pubblica che, in quanto tali, beneficiano del patrocinio (e della rappresentanza e dell'assistenza in giudizio) da parte dell'Avvocatura dello Stato (ai sensi del regio decreto 30 ottobre 1933, n. 1611).

Nel corso dell'esame in **sede referente** è stato previsto – tra le disposizioni finali (**comma 10-*bis***) - che la prima relazione al Parlamento (di cui all'articolo 14, comma 1) venga trasmessa entro il **30 novembre 2022**.

Inoltre, è stato aggiunto che entro il **31 ottobre 2022** il Presidente del Consiglio dei ministri è tenuto a trasmettere al Parlamento una relazione che dia conto dell'attuazione al 30 settembre 2022 delle disposizioni di cui al decreto-legge in esame, anche al fine di formulare eventuali proposte in merito.

Infine, il **comma 10-*ter***, introdotto nel corso dell'esame in sede referente, dispone che tutti i **pareri delle Commissioni parlamentari e del Copasir**, previsti dal decreto-legge in esame, anche all'esito delle modifiche introdotte in sede di conversione, devono essere resi **entro il termine di 30 giorni dalla trasmissione dei relativi schemi** di decreto. Trascorso inutilmente il termine, si può comunque procedere all'adozione dei relativi provvedimenti.

Articolo 18
(Disposizioni finanziarie)

L'**articolo 18** detta disposizioni relative alla copertura finanziaria relativa alla istituzione dell'Agenzia per la cybersicurezza nazionale.

A tal fine apposta in un capitolo dedicato dello stato di previsione del Ministero dell'economia e delle finanze - al quale si prevede affluiscano,

altri proventi patrimoniali e di gestione, i proventi delle sanzioni irrogate dall'Agenzia (cfr. *supra* l'articolo 11, comma 2 del decreto-legge).

La dotazione del capitolo di bilancio dedicato all'Agenzia è, ad ogni modo, pari a:

- 2 milioni per il 2021;
- 41 milioni per il 2022;
- 70 milioni per il 2023;
- 84 milioni per il 2024;
- 100 milioni per il 2025;
- 110 milioni per il 2026;
- 122 milioni a decorrere dall'anno 2027.

A tali oneri si provvede mediante corrispondente riduzione del Fondo per far fronte ad esigenze indifferibili che si manifestano nel corso della gestione, istituito (ai sensi dell'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190) sullo stato di previsione del Ministero sopra ricordato.

A tale Fondo si prevede affluiscano, in via incrementale, le risorse iscritte sui bilanci delle amministrazioni interessate, correlate alle funzioni attribuite all'Agenzia, le quali sono accertate, anche in conto residui, con decreto del Ministro dell'economia e delle finanze (di concerto con i Ministri responsabili).

Articolo 19
(Entrata in vigore)

L'**articolo 19** dispone che il decreto-legge entri in vigore il giorno successivo a quello della sua pubblicazione in Gazzetta Ufficiale.

Il decreto-legge è dunque vigente dal **15 giugno 2021**.

QUADRO NORMATIVO

L'attuazione della direttiva NIS sulla sicurezza delle reti e dei sistemi informativi

Negli ultimi anni, per fronteggiare il fenomeno in espansione, sono state adottate misure per la tutela delle reti, a livello nazionale e internazionale, in maniera diffusa e sempre più penetrante.

A livello di Unione europea la direttiva (UE) 2016/1148 del 6 luglio 2016 reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. **direttiva NIS** - *Network and Information Security*) al fine di conseguire un "livello elevato di **sicurezza della rete e dei sistemi informativi** in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea".

Il decreto legislativo n. 65 del 18 maggio 2018, che ha recepito la direttiva NIS, detta la **cornice legislativa** delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva.

In particolare, al **Presidente del Consiglio dei ministri** compete l'adozione, sentito il Comitato interministeriale per la sicurezza della Repubblica - CISR (il DL 82/2019 ha sostituito il parere del CISR con quello del CIC), della **strategia nazionale di sicurezza cibernetica** per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Con la medesima procedura sono adottate linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica (art. 6).

La qualifica di **Autorità nazionale competente NIS** viene attribuita con il D.L. 82/2021 all'Agenzia per la cybersicurezza nazionale. Nella versione previgente non era prevista una autorità nazionale NIS, ma ciascun ministero e, per taluni ambiti, ciascuna regione, era definito autorità competenze NIS per il settore di competenza. Nella nuova versione, i singoli ministeri sono designati quali **autorità di settore** in base al settore di competenza (Ministero dello sviluppo economico, Ministero delle infrastrutture e della mobilità sostenibili, Ministero dell'economia e delle finanze, Ministero della salute, Ministero della transizione ecologica). Tali autorità sono i soggetti competenti per settore (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali) in materia di sicurezza delle reti e dei sistemi informativi. L'Autorità nazionale competenze NIS verifica l'applicazione della direttiva a livello nazionale (art. 7).

Presso la Presidenza del Consiglio dei ministri è istituito (art. 8) il ***Computer Emergency Response Team*** **CSIRT italiano** (ridenominato **CSIRT Italia** dal DL 82/2021), con lo stanziamento di specifiche risorse finanziarie, al quale sono attribuite – a decorrere dall'entrata in vigore del relativo decreto di organizzazione e funzionamento adottato con il DPCM 8 agosto 2019 - le funzioni del CERT

nazionale (presso il Ministero per lo sviluppo economico) e del CERT-PA (presso l'Agenzia per l'Italia digitale-AGID). Il CSIRT è definito dalla direttiva 2016/1148 quale "gruppo di intervento per la sicurezza informatica in caso di incidente", che ogni Stato membro è chiamato a designare con il compito di trattare gli incidenti e i rischi secondo una procedura definita.

Viene designato il Dipartimento delle informazioni per la sicurezza (DIS) quale **punto di contatto unico (**funzione ora trasferita dal DL 82/2021 all'Agenzia per la cybersicuezza), organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea (art, 7, comma 3).

L'**autorità di contrasto** è individuata nell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (Polizia postale) al quale è attribuita la competenza ad assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate (art. 3, comma 1, lett. d).

Gli **operatori di servizi essenziali**, ai fini del provvedimento, sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), individuati dalle autorità competenti NIS.

Il decreto definisce inoltre gli **obblighi** in capo agli **operatori dei servizi essenziali e ai fornitori dei servizi digitali** con riferimento alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall'allegato III. È posto a loro carico l'obbligo di individuare le misure tecniche e organizzative relative alla gestione dei rischi, alle misure per prevenire e minimizzare gli impatti degli incidenti e, sotto il profilo procedurale, sono definite le modalità di notifica degli incidenti che abbiano un impatto rilevante sui servizi forniti individuando altresì le condizioni e le modalità secondo le quali potranno essere coinvolti gli organismi di altri Paesi (art. 4).

Sono poi individuati i **poteri di controllo delle autorità NIS** sia nei confronti degli operatori di servizi essenziali, che dei fornitori di servizi digitali anche prevedendo poteri di verifica e di ispezione oltre che l'irrogazione di sanzioni amministrative nel caso di mancato adempimento degli obblighi previsti.

Il 16 dicembre 2020 la Commissione europea ha adottato una proposta di nuova direttiva sulla sicurezza delle reti e dei sistemi informativi la cosiddetta direttiva NIS 2.

La proposta mira a colmare le carenze della precedente direttiva NIS, per adattarla alle esigenze attuali. A tal fine, la proposta della Commissione amplia il campo di applicazione dell'attuale direttiva NIS aggiungendo nuovi settori in base alla loro criticità per l'economia e la società e introducendo un limite di dimensione, il che significa che saranno incluse tutte le medie e grandi aziende in settori selezionati. Allo stesso tempo, lascia agli Stati membri una certa flessibilità nell'identificare entità più piccole con un profilo di rischio elevato per la sicurezza (*sul punto si veda altresì il paragrafo* Documenti all'esame dell'UE).

La definizione del perimetro di sicurezza cibernetica

Il perimetro di sicurezza cibernetica è stato istituito e disciplinato dal **decreto-legge n. 105 del 2019**. Successivamente, il **decreto-legge n. 162 del 2019**, recante proroga di termini e ulteriori disposizioni in materia di p.a., ha apportato (art. 27) alcune modifiche al decreto-legge n. 105 del 2019 con particolare riguardo alle procedure e alle modalità per la definizione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica.

Il decreto-legge n. 105 del 2019 ha istituito il **Perimetro di sicurezza nazionale cibernetica (PSNC)** al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati necessari allo svolgimento di funzioni o alla prestazione di servizi, dalla cui discontinuità possa derivare un pregiudizio alla sicurezza nazionale.

Con tale provvedimento sono state previste una serie di altre misure volte a garantire i necessari *standard* di sicurezza rivolti a minimizzare i rischi alla sicurezza cibernetica.

La **determinazione** puntuale dei **soggetti inclusi nel perimetro** è affidata ad un **atto amministrativo del Presidente del Consiglio dei ministri**, come stabilito dal D.L. 162/2019, anziché ad un DPCM, come originariamente previsto dal decreto-legge n. 105. Ciò in ragione del fatto che "l'elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, considerato nella sua interezza, presenta particolari profili di sensibilità sotto il profilo della sicurezza". Per tali motivi, l'atto amministrativo, per il quale è escluso dal diritto di accesso, non è soggetto a pubblicazione.

Il medesimo D.L. 162/2019 ha rinviato ad un DPCM la definizione:

- delle **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 (art. 1, comma 2, lett. a), D.L. 162/2019);
- dei **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 (art. 1, comma 2, lett. b), D.L. 162/2019).

In attuazione di tale disposizione il Governo ha adottato il DPCM 30 luglio 2020, n. 131 (pubblicato nella G.U. 21 ottobre 2020, n. 261) che ha dato avvio alla concreta realizzazione del PSCN.

Dopo la pubblicazione del DPCM 131/2020 è stato adottato infatti un primo elenco dei soggetti inclusi nel perimetro di sicurezza cibernetica (22 dicembre 2020).

Successivamente, il 15 giugno 2021, il Presidente del Consiglio, a seguito della proposta formulata dal Comitato interministeriale per la sicurezza della Repubblica (CISR), ha firmato l'aggiornamento dell'elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica. È stato, così, previsto un allargamento dell'ambito di applicazione del perimetro ad ulteriori soggetti pubblici e privati che, complessivamente, esercitano, attraverso reti, sistemi informativi e servizi informatici, 223 funzioni essenziali dello Stato, ovvero erogano servizi essenziali per il mantenimento di attività civili, sociali o economiche strategiche. Allo stesso tempo, si è provveduto ad un affinamento di alcune funzioni e servizi essenziali dello Stato già ricompresi nel perimetro (Comunicato della Presidenza del Consiglio dei ministri 15 giugno 2021).

Ai sensi dell'art. 1, comma 2, lett. b), del DL 105/2019, entro i 6 mesi successivi alla comunicazione della avvenuta inclusione nel PSNC, le amministrazioni interessate **trasmettono gli elenchi delle reti, dei sistemi informativi e dei servizi informatici** di rispettiva pertinenza alla Presidenza del Consiglio dei ministri (soggetti pubblici) e al MISE (soggetti privati). Il DL in esame prevede la trasmissione, in luogo di tali due organi, all'Agenzia per la cybersicurezza nazionale. Successivamente, gli elenchi vengono inoltrati alla Polizia postale e delle comunicazioni, organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazioni.

Una volta che gli elenchi sono trasmessi all'Agenzia, il PSNC diviene operativo nei confronti dei soggetti inseriti, che pertanto sono tenuti a **notificare gli eventuali incidenti su reti, sistemi informatici e servizi informatici** al Gruppo di intervento per la difesa informatica in caso di incidente (**CSIRT Italia**). Lo CSIRT inoltra tali notifiche al DIS (ora all'Agenzia) e alla Polizia postale.

Gli stessi soggetti inseriti nel perimetro sono tenuti ad applicare le previste **misure di sicurezza cibernetica** (art. 1, comma 3, DL 105/2019).

La tassonomia degli incidenti da notificare, le procedure di notifica e le misure di sicurezza sono state definite con il DPCM 14 aprile 2021, n. 81 (pubblicato nella GU 11 giugno 2021, n. 138) emanato in attuazione dell'art. 1, comma 3 del DL 105/2019.

Il D.L. 105/2019 interviene inoltre sulle **procedure, modalità e termini** ai quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, che intendano procedere all'**affidamento di forniture di beni, sistemi e servizi ICT**, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici. Il Centro di valutazione e certificazione nazionale (**CVCN**) può effettuare verifiche preliminari e imporre condizioni e test di *hardware* e *software* (art. 1, comma 6, DL 105/2019).

Le procedure di affidamento, verifica, ispezione e test sono definiti con specifico regolamento adottato con il DPR 5 febbraio 2021, n. 54 in attuazione dell'art. 1, comma 6, DL 105/2019.

Il Presidente del Consiglio dei ministri **trasmette alle Camere una relazione** sulle attività svolte dopo l'adozione di tale regolamento (art. 1, comma 19-bis, DL 105/2019).

Il **Ministero dell'interno** e il **Ministero della difesa**, in relazione alla specificità delle loro forniture di beni e servizi ICT possono utilizzare propri Centri di valutazione (CEVA) impiegando le metodologie definite dal CVCN. In tali casi informano il CVCN con modalità stabilite da un DPCM (ancora da adottare). Non sono oggetto di comunicazione gli affidamenti di forniture per l'accertamento e la repressione dei reati e altri casi di deroga stabiliti con regolamento (art. 1, comma 6, DL 105/2019).

Sono poi individuati alcuni **compiti** del Centro di valutazione e certificazione nazionale (**CVCN**), con riferimento all'**approvvigionamento** di prodotti, processi, servizi di tecnologie dell'informazione e della comunicazione (ICT) e associate infrastrutture - qualora destinati a reti, sistemi informativi, sistemi informatici ricompresi nel perimetro di sicurezza nazionale cibernetica. Tra questi compiti, il CVCN procede alla verifica delle condizioni di sicurezza attraverso test, anche avvalendosi di laboratori accreditati secondo criteri stabiliti con DPCM.

Al contempo sono determinati alcuni **obblighi** per: gli operatori dei servizi essenziali; i fornitori di servizi digitali; le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, inclusi nel perimetro di sicurezza nazionale cibernetica (art. 1, comma 7, DL 105/2019).

È altresì previsto che il Presidente del Consiglio - su deliberazione del CISR (compito non trasferito al CIC dal DL 82/2021) - 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**. Entro 30 giorni il Presidente del Consiglio è tenuto a informare il Comitato parlamentare per la sicurezza della Repubblica (Copasir) delle misure disposte (art. 5 DL 105/2019).

Al Presidente del Consiglio dei ministri è affidato inoltre il coordinamento della coerente attuazione delle disposizioni del decreto-legge che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del DIS (ora dell'Agenzia) che assicura gli opportuni raccordi con le autorità titolari delle attribuzioni e con i soggetti coinvolti (art. 1, comma 19-bis, DL 105/2019).

Il provvedimento reca quindi un articolato **sistema sanzionatorio** per i casi di violazione degli obblighi ivi previsti ed individua le **autorità competenti** all'accertamento delle violazioni e all'irrogazione delle **sanzioni** (art. 1, commi 9-14, DL 105/2019).

Per completezza, infine, si ricorda che è stata disposta l'istituzione della **Direzione generale per lo sviluppo della prevenzione e tutela informatiche**

presso il Dipartimento della pubblica sicurezza del Ministero dell'interno ad opera del decreto-legge 34/2020 (cd. decreto Rilancio, art. 240).

A tale direzione generale sono attribuiti:

- lo sviluppo della **prevenzione e tutela informatica e cibernetica** (quale struttura per la sicurezza e per la regolarità dei servizi di telecomunicazione, preposta ad assicurare i servizi di protezione informatica ed i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate;
- lo sviluppo delle attività attribuite al Ministero dell'interno in materia di **perimetro di sicurezza nazionale cibernetica**;
- l'unità di indirizzo e **coordinamento delle attività svolte dalla polizia postale e delle comunicazioni**, specialità della Polizia di Stato - e degli altri compiti che costituiscano il completamento di supporto alle attività investigative.

DOCUMENTI ALL'ESAME DELLE ISTITUZIONI DELL'UE

Proposte normative nel contesto della nuova Strategia dell'UE per la cibersicurezza

Nel dicembre 2020 la Commissione europea e il Servizio europeo per l'azione esterna (SEAE) hanno presentato una nuova Strategia dell'UE per la cybersicurezza, che include proposte per l'introduzione di strumenti **normativi**, **strategici** e di **investimento**.

Sul tema il 22 marzo 2021 il Consiglio ha adottato conclusioni, con le quali, tra l'altro, si sottolinea il ruolo essenziale della cybersicurezza per la transizione **verde e digitale** e la necessità di realizzare l'obiettivo dell'autonomia strategica mantenendo nel contempo un'economia aperta.

In tale contesto, la Commissione europea ha presentato **due proposte normative per contrastare** i rischi attuali e futuri online e offline:

- una proposta di direttiva aggiornata per proteggere meglio la **rete** e i **sistemi informativi;**
  La normativa sostituirebbe l'attuale direttiva NIS per affrontarne le carenze che nel suo periodo di applicazione sono state riscontrate. In particolare il nuovo regime espanderebbe l'applicazione di quello attuale aggiungendo nuovi settori in base alla loro criticità per l'economia e la società e introducendo un requisito relativo alle dimensioni: sono incluse tutte le **medie** e **grandi imprese** operanti in settori selezionati. Tuttavia gli Stati membri godono di una certa flessibilità per individuare soggetti più piccoli con un profilo di rischio per la sicurezza elevato.
  La proposta elimina la distinzione tra gli operatori di **servizi essenziali** e i fornitori di **servizi digitali;** il considerando 7) della direttiva sottolinea che tale differenziazione si è rivelata obsoleta, in quanto non riflette l'effettiva importanza dei settori o dei servizi per le attività sociali ed economiche nel mercato interno.
  La proposta di direttiva, inoltre, rafforza e razionalizza gli obblighi delle imprese in materia di sicurezza e comunicazione. La Commissione propone altresì di affrontare la questione relativa alla sicurezza delle **catene di approvvigionamento** e delle relazioni tra i fornitori. Gli Stati membri, in collaborazione con la Commissione e l'ENISA (l'agenzia dell'Unione europea per la cybersicurezza), possono effettuare valutazioni coordinate dei rischi delle catene di approvvigionamento critiche, basandosi sull'approccio adottato nel contesto della raccomandazione della Commissione sulla cybersicurezza delle reti 5G. La proposta introduce misure di vigilanza più rigorose per le autorità nazionali e prescrizioni di applicazione più rigide, e mira ad armonizzare i regimi sanzionatori in tutti gli Stati membri. È infine rafforzato il ruolo del gruppo di cooperazione anche tramite una maggiore condivisione delle informazioni tra le autorità degli Stati membri.
  La proposta della Commissione riguarda i seguenti **settori** e **sottosettori**:

  - **soggetti essenziali**: energia (energia elettrica, teleriscaldamento e teleraffrescamento, petrolio, gas e idrogeno), trasporto (aereo, ferroviario, per vie d'acqua e su strada), settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fabbricazione di prodotti farmaceutici e di dispositivi medici

critici, acqua potabile, acque reflue, infrastrutture digitali (punti di interscambio Internet, fornitori di servizi DNS, registri dei nomi di dominio di primo livello, fornitori di servizi di *cloud computing*, fornitori di servizi di *data center*, reti per la consegna dei contenuti, prestatori di servizi fiduciari, reti pubbliche di comunicazione elettronica e servizi di comunicazione elettronica), pubblica amministrazione e settore spaziale;

- **soggetti importanti**: servizi postali e di corriere, gestione dei rifiuti, sostanze chimiche, settore alimentare, fabbricazione di altri dispositivi medici, computer ed elettronica, macchinari e apparecchiature, veicoli a motore e fornitori di servizi digitali (mercati online, motori di ricerca online e piattaforme di social network).

- una nuova direttiva sulla resilienza delle entità critiche**.**
  La proposta espande l'ambito di applicazione della direttiva in materia di infrastrutture critiche (di cui si dispone l'abrogazione). Allo stato il regime vigente riguarda solo i settori dell'energia e dei trasporti, mentre la nuova proposta contempla **10 settori**: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. Il nuovo regime tiene conto sia dei **rischi naturali** sia di quelli di **origine umana**, compresi gli incidenti, le calamità naturali, le minacce antagoniste, i reati terroristici, e le emergenze di sanità pubblica come le **pandemie**. Gli Stati membri sono obbligati ad adottare una strategia volta a garantire la resilienza dei soggetti critici, effettuare una **valutazione multirischio** e designare **referenti nazionali** e autorità competenti. In particolare sulla base della valutazione dei rischi, ciascuno Stato membro individua i soggetti critici nei diversi settori. I soggetti critici sono a loro volta tenuti a effettuare una propria **valutazione** dei **rischi**, che tenga conto della valutazione dei rischi a livello nazionale e delle specificità e delle condizioni locali. Tali soggetti adottano quindi misure tecniche e organizzative volte a rafforzare la loro resilienza e forniscono informazioni alle autorità competenti per quanto riguarda gli incidenti e i potenziali incidenti.

LA CYBERSECURITY IN FRANCIA, GERMANIA E REGNO UNITO

Francia

Nell'ottobre 2015 è stata annunciata la **Strategia nazionale per la sicurezza digitale** (*Stratégie nationale pour la sécurité du numérique*), diretta a sostenere la transizione digitale della società francese.

La Strategia è caratterizzata da **cinque obiettivi**:

1. Garantire la sovranità della Francia e assicurare la sicurezza delle sue infrastrutture critiche nel caso di un grande attacco informatico. Questo obiettivo è perseguito rafforzando le capacità scientifiche, tecniche e industriali necessarie e la sicurezza delle infrastrutture vitali;
2. Proteggere i cittadini e le imprese e combattere la criminalità informatica. In questa direzione è promosso il percorso "*identité numérique*", allo scopo di rafforzare la fiducia degli utenti nella loro vita digitale, limitando il rischio di uno sfruttamento indesiderato dei loro dati, e creare altresì un dispositivo nazionale di assistenza alle vittime di atti di cyber-violenza;
3. Sensibilizzare i ragazzi sulla sicurezza digitale e sui comportamenti responsabili nel cyberspazio, a partire dall'età scolastica. Anche l'istruzione superiore e la formazione continua devono comprendere una sezione dedicata alla *sécurité numérique*;
4. Sviluppare un ecosistema favorevole alla ricerca e all'innovazione e rendere la sicurezza digitale un fattore di competitività. La Francia sostiene lo sviluppo dell'economia e la promozione internazionale dei suoi prodotti e servizi digitali e garantisce la disponibilità di prodotti e servizi digitali con livelli di fiducia e sicurezza adeguati agli usi e alle minacce informatiche;
5. Promuovere la cooperazione con gli Stati membri volontari in modo da favorire un'Autonomia strategica digitale europea (*Autonomie stratégique numérique européenne*), giocando un ruolo attivo nella promozione di un cyberspazio sicuro, stabile e aperto.

Dal punto di vista operativo, i cinque obiettivi possono essere raggiunti grazie alla partecipazione di diversi soggetti.

Un ruolo fondamentale è svolto dall'**Agenzia nazionale della sicurezza dei sistemi di informazione** (*Agence Nationale de la Sécurité des Systèmes d'Information*, *ANSSI*), che è il soggetto primario incaricato di misurare e valutare i rischi e gli effetti degli attacchi informatici, rivolti sia ai soggetti pubblici sia ai privati.

Il ruolo dell'ANSSI è quello di promuovere una risposta coordinata ed efficiente ai problemi di della sicurezza digitale in Francia.

L'Agenzia, istituita con il *Décret n. 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé «Agence nationale de la sécurité des systèmes d'information»*, svolge in particolare le seguenti funzioni:

- assicura la funzione di autorità nazionale per la difesa dei sistemi di informazione. In questa veste, propone al Primo ministro misure per

rispondere alle crisi che incidono o minacciano la sicurezza dei sistemi di informazione delle autorità pubbliche e degli operatori di vitale importanza e coordina, nel quadro degli orientamenti stabiliti dal Primo ministro, l'azione del governo in materia di difesa dei sistemi di informazione;
- anima e coordina i lavori interministeriali sulla sicurezza dei sistemi informativi;
- elabora le misure di protezione dei sistemi di informazione proposti al Primo ministro. Assicura l'applicazione delle misure adottate;
- effettua ispezioni dei sistemi informativi dei servizi statali e degli operatori pubblici o privati;
- implementa dispositivi di rilevamento degli eventi che possono influire sulla sicurezza dei sistemi di informazione dello Stato, delle autorità pubbliche e degli operatori pubblici e privati, e coordina la risposta a tali eventi;
- raccoglie le informazioni tecniche relative agli incidenti che interessano i sistemi di informazione di tali soggetti; può inoltre aiutare a rispondere a questi incidenti;
- rilascia le approvazioni per dispositivi e meccanismi di sicurezza destinati a proteggere, nei sistemi di informazione, le informazioni coperte dal segreto di difesa nazionale;
- partecipa ai negoziati internazionali e collabora con le controparti straniere;
- assicura la formazione del personale qualificato nel campo della sicurezza dei sistemi di informazione

(art. 3 del Decreto del 2009, come modificato dall'art. 7 del *Décret n. 2020-455 du 21 avril 2020 portant création d'un service à compétence nationale dénommé «opérateur des systèmes d'information interministériels classifiés»*[1])

L'ANSSI fa riferimento al Segretario della difesa e della sicurezza nazionale (*Secrétaire général de la défense et de la sécurité nationale*), che assiste il Primo ministro nell'esercizio delle sue responsabilità in materia di difesa e sicurezza.

La Direzione dell'ANSSI è affidata a un Direttore generale, nominato dal Primo ministro. L'ANSSI è articolata in quattro Sottodirezioni:

1. Sottodirezione Amministrazione (*Sous-direction Administration*, SDA);
2. Sottodirezione Expertise (*Sous-direction Expertise*, SDE);
3. Sottodirezione Operazioni (*Sous-direction Opérations*, SDO);
4. Sottodirezione Strategia (*Sous-direction Stratégie*, SDS).

All'interno della SDO opera il Centro governativo di vigilanza, allerta e risposta agli attacchi informatici (*Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*, CERT-FR), che fornisce supporto nella gestione degli incidenti a ministeri, istituzioni, giurisdizioni, autorità indipendenti, collettività territoriali e OIV (operatori di importanza vitale). È responsabile dell'assistenza agli organi

[1] Il decreto istituisce, nella forma di un servizio di competenza nazionale presso il Segretario generale della Difesa e della Sicurezza nazionale, un operatore di sistemi informativi interministeriali classificati. Questo operatore è il risultato della fusione del centro comunicazioni governativo (*centre de transmissions gouvernemental*) - un organismo militare alle dipendenze organiche del Capo di Stato Maggiore della Difesa e posto sotto l'autorità del Segretario Generale della Difesa e della Sicurezza Nazionale - e la Sottodirezione digitale (*Sous-direction du numérique*) che dipendeva all'Agenzia nazionale per la sicurezza dei sistemi informativi. La creazione di questo operatore ha lo scopo di razionalizzare l'impiego di dati classificati, di ottimizzare il servizio fornito alle autorità e di facilitare la convergenza tecnologica dei sistemi implementati. L'operatore assicura inoltre la funzione di direzione dei sistemi di informazione per tutti gli organismi che compongono il Segretariato generale della difesa e della sicurezza nazionale.

dell'amministrazione nell'attivare i mezzi di protezione necessari. Esso svolge funzioni di CERT (*computer emergency response team*) nazionale[2].

Ai sensi dell'art. L. 2321-1 del codice della difesa (inserito dalla *Loi n. 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*), nel quadro della strategia di sicurezza nazionale e della politica di difesa, il Primo ministro definisce la politica e coordina l'azione del Governo in materia di sicurezza e di difesa dei sistemi di informazione. Egli a tal fine ha a sua disposizione l'autorità nazionale di sicurezza dei sistemi di informazione.

La *Loi n. 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense* ha fissato gli orientamenti relativi alla politica di difesa e ha indicato la programmazione militare per il periodo 2019-2015. In materia di cybersicurezza, la legge consente agli operatori di comunicazioni elettroniche, per le esigenze della difesa e della sicurezza dei sistemi di informazione, di istituire dispositivi che consentano, a partire da marcatori tecnici, di rilevare gli eventi che possono incidere sulla sicurezza dei sistemi di informazione dei loro abbonati. Quando viene a conoscenza di una minaccia, l'ANSSI può chiedere a questi operatori di sfruttare i marcatori di attacco informatico che fornirà loro (art. L. 33-14 del codice delle poste e delle comunicazioni elettroniche, inserito dalla legge n. 2018-607).

L'ANSSI coordina i **Centri per la valutazione della sicurezza dell'informazione** (*Centres d'Évaluation de la Sécurité des Technologies de l'Information*, CESTI) che sono fornitori di servizi volti a certificare la sicurezza dei prodotti[3]. Un prodotto per essere certificato deve rispettare le regole del regime di certificazione francese, che permette due tipi di valutazione:

- la conformità al livello di garanzia della valutazione[4];
- la certificazione della sicurezza di primo livello (*Certification de Sécurité de Premier Niveau*, CSPN) dei prodotti informatici, istituita dall'ANSSI nel 2008.

L'ANSSI dispone inoltre di un proprio centro di formazione, il **Centro di formazione sulla sicurezza dei sistemi di informazione** (*Centre de formation à la sécurité des systèmes d'information*, CFSSI), che in particolare rilascia un Diploma di esperto in sicurezza dei sistemi di informazione (ESSI) riconosciuto come titolo di livello 1 e registrato nel Repertorio nazionale delle certificazioni professionali.

Un altro soggetto di notevole rilevanza è la **Commissione nazionale dell'informatica e delle libertà** (*Commission Nationale de l'Informatique et des Libertés*, CNIL), istituita con la legge n. 78-17 (*Loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*).

La CNIL è un'autorità amministrativa indipendente che è responsabile di garantire che l'informatica sia al servizio del cittadino e che non violi l'identità e i diritti umani, la privacy, la libertà individuale e quella pubblica. La CNIL analizza le ripercussioni delle

[2] I CERT sono organismi incaricati di raccogliere le segnalazioni di incidenti informatici e potenziali vulnerabilità nei software che provengono dalla comunità degli utenti interessati.

[3] Si veda anche il *Décret n° 2002-535* du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, relativo alla certificazione francese per i prodotti e i sistemi di sicurezza.

[4] La *Evaluation Assurance Level* (livello di garanzia della valutazione) di un prodotto o sistema elettronico è un valore numerico che esprime una valutazione di sicurezza basata sui *Common Criteria*, standard internazionale in vigore dal 1999, poi riconosciuto dall'ISO mediante la ISO/IEC 15408. Il prodotto valutato, detto "TOE" (*Target of Evaluation*, in italiano ODV, oggetto della valutazione), può essere hardware, software o entrambi. Può variare da un minimo di EAL1 a un massimo di EAL7.

innovazioni tecnologiche sulla privacy e sulla libertà e collabora con gli analoghi soggetti europei e internazionali per sviluppare una regolamentazione armonizzata.

La Commissione si compone di un collegio multidisciplinare di diciotto membri, di cui:

- 4 parlamentari (2 deputati, 2 senatori);
- 2 membri del Consiglio economico, sociale e ambientale;
- 6 rappresentanti dei tribunali superiori (2 consiglieri di stato, 2 consiglieri della Corte di cassazione, 2 consiglieri della Corte dei conti);
- 5 persone qualificate designate dal Presidente dell'Assemblea nazionale (1 personalità), dal Presidente del Senato (1 personalità), dal Consiglio dei ministri (3 personalità). Il mandato dei commissari è di cinque anni o, per i parlamentari, di durata pari alla loro carica elettiva;
- il presidente della CADA (Commissione di accesso ai documenti amministrativi).

Il Presidente della CNIL è nominato con decreto del Presidente della Repubblica, tra i membri della Commissione stessa, il suo mandato è di cinque anni.

Le sue **missioni principali** sono:

1. Informare e proteggere i diritti. Svolge azioni di comunicazione pubblica attraverso la stampa, il sito web, la presenza sui social network o fornendo strumenti pedagogici. Può essere direttamente interpellata da organismi, società o istituzioni per condurre azioni di formazione e sensibilizzazione sul RGPD (Regolamento generale sulla protezione dei dati)[5], la CNIL partecipa anche a mostre o conferenze per informare e allo stesso tempo informarsi. Essa garantisce che i cittadini possano accedere efficacemente ai dati contenuti nei trattamenti che li riguardano. Chiunque può contattare la CNIL in caso di difficoltà nell'esercizio dei propri diritti inviando un reclamo concernente:

- la reputazione online;
- il commercio;
- le risorse umane;
- le banche e il credito;

2. Accompagnare e consigliare. Nel quadro del RGPD, la conformità è un indicatore di buona *governance*, che soddisfa la sfida della reputazione, della fiducia e costituisce un vantaggio competitivo per le aziende. Per aiutare gli organismi pubblici e privati a prepararsi all'implementazione del RGPD, la CNIL offre una serie di strumenti completa e adattata alle loro dimensioni ed esigenze. Le attività di consulenza e regolamentazione della CNIL sono varie: pareri su progetti di testi provenienti dal Governo riguardanti la protezione dei dati personali o la creazione di nuovi archivi, consigli, partecipazione alle audizioni parlamentari. Nell'ambito di questa attività, la CNIL assicura la ricerca di soluzioni che consentano agli organismi pubblici e privati di perseguire i loro legittimi obiettivi nel rigoroso rispetto dei diritti e delle libertà dei cittadini.

3. Anticipare e innovare. Partecipa alla costituzione di un dibattito sociale sulle questioni etiche dei dati. È un punto di contatto e di dialogo con gli ecosistemi dell'innovazione digitale (ricercatori, start-up, laboratori). Contribuisce allo sviluppo di

[5] Il regolamento generale sulla protezione dei dati (in inglese *General Data Protection Regulation*) è il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. Adottato il 27 aprile 2016, esso è entrato in vigore il 25 maggio dello stesso anno e operativo a partire dal 25 maggio 2018.

soluzioni tecnologiche che tutelino la privacy, consigliando le aziende il più direttamente possibile, nello spirito della *privacy by design*[6].

Per contribuire ai dibattiti sul digitale, la CNIL ha lanciato LINC, un laboratorio di innovazione digitale, con riflessioni prospettiche, condivisione e sperimentazione in materia.

Al fine di rafforzare la sua missione di monitoraggio e di riflessione, la CNIL guida un comitato di esperti esterni (*Comité de la prospective*) composto da ventitre membri con profili e background diversi: sociologi, economisti, antropologi, filosofi, imprenditori, ricercatori, autori, giuristi, giornalisti.

La *Loi n. 2016-1321 du 7 octobre 2016 pour une République numérique* ha affidato alla CNIL la missione di condurre una riflessione sulle questioni etiche e le questioni sociali sollevate dall'evoluzione delle tecnologie digitali (v. *Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle*, dicembre 2017).

4. Controllare e sanzionare. Il controllo successivo costituisce un mezzo privilegiato di intervento presso i gestori del trattamento dei dati personali. Permette alla CNIL di verificare in loco l'attuazione concreta della legge. Il programma dei controlli è elaborato in base ai temi di attualità e delle principali problematiche di cui viene interessata la CNIL.

Il Presidente della CNIL ha la possibilità di sollecitare gli organismi che non rispettano le disposizioni del RGDP o della legge a conformarsi entro un dato periodo. Tali comunicazioni formali possono essere rese pubbliche in base alla gravità delle violazioni accertate o al numero di persone interessate.

Dopo il controllo o i reclami, in caso di violazione delle disposizioni del RGPD o della legge da parte dei responsabili del trattamento e dei subappaltatori, la formazione ristretta della CNIL può imporre sanzioni ai responsabili di trattamenti che non rispettano le norme.

La formazione ristretta del CNIL è composta da 5 membri e un Presidente distinto dal Presidente della CNIL.

In base al RGPD, l'ammontare delle sanzioni pecuniarie può arrivare fino a 20 milioni di euro o, nel caso di un'impresa, fino al 4% del fatturato annuale globale. Queste sanzioni possono essere rese pubbliche.

Quando le violazioni del RGPD o della legge vengono portate alla sua attenzione, la formazione ristretta della CNIL può:

- pronunciare un richiamo all'ordine;
- ingiungere di rendere il trattamento conforme;
- limitare temporaneamente o permanentemente un trattamento;
- sospendere i flussi di dati;
- ordinare di soddisfare le richieste per l'esercizio dei diritti delle persone;
- pronunciare una sanzione amministrativa.

Dalla data di notifica della decisione della formazione ristretta, l'organizzazione coinvolta ha un periodo di due mesi per presentare appello al Consiglio di Stato contro la decisione della CNIL.

Per quanto concerne i **centri pubblici di ricerca**, molti sforzi sono stati dedicati alla sicurezza digitale. In particolare, il CNRS (*Centre National de la Recherche Scientifique*)

[6] In base al principio della *privacy by design* la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali deve comportare l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione sia dell'esecuzione del trattamento medesimo.

ha dedicato l'anno 2016 alla sicurezza e ha creato un gruppo di ricerca (*Groupement De Recherche*, GDR) specifico sulla sicurezza digitale.

Il *GDR Sécurité Informatique* è uno strumento di stimolo per la ricerca scientifica. Gli argomenti trattati dal GDR comprendono la crittografia, la protezione della privacy, la sicurezza dei dati multimediali, la sicurezza di reti e infrastrutture, la sicurezza dei sistemi software e hardware e i metodi formali per la sicurezza.

Il GDR organizza annualmente vari eventi, tra i quali:

- le "giornate nazionali" presso la sede CNRS di Parigi, che riuniscono oltre 200 scienziati. Le giornate nazionali consistono in sessioni plenarie con presentazioni a livello di comunità e sessioni parallele dei gruppi di lavoro;
- una scuola estiva in cybersicurezza, principalmente per i giovani ricercatori che affrontano per una settimana alcuni argomenti sulla sicurezza informatica. Circa 40 giovani ricercatori frequentano ogni anno la scuola;
- una settimana di incontri tra aziende e studenti di dottorato (*Rencontres Entreprises-DOCtorants en Sécurité*, REDOCS), organizzata ogni anno in autunno nel campus CNRS di Gif-sur-Yvette, allo scopo di mettere in contatto i dottorandi con i principali attori economici nel campo della sicurezza informatica.

È stato infine previsto, agli inizi del 2021, un **piano da 1 miliardo di euro per rafforzare la cybersecurity.** Finanziata attraverso il piano adottato dal governo Francese per uscire dalle difficoltà economiche legate al Covid-19 (*Plan de Relance*) e attraverso il *Programme d'investissement d'avenir*, *la* ***stratégie nationale pour la cybersécurité,*** mira, tra l'altro, a raddoppiare la forza lavoro nel settore entro il 2025. La transizione al digitale è portatrice di progresso, ma gli spazi digitali sono anche sede di azioni criminali, in particolare di attacchi informatici. Per far fronte a questa minaccia, il governo ha quindi annunciato l'intenzione di mobilitare **1 miliardo di euro, di cui 720 milioni di sussidi pubblici**. La nuova ***strategia nazionale per la sicurezza informatica*** mira, in particolare a far emergere **i campioni francesi** della sicurezza informatica.

Tra i **principali obiettivi fissati per il 2025** si segnalano i seguenti:

- triplicare il fatturato del settore (da 7,3 miliardi a 25 miliardi di euro);
- posizionare la Francia rispetto alla concorrenza internazionale, in particolare raddoppiando i posti di lavoro nel settore (da 37.000 a 75.000);
- strutturare il settore e riposizionare la Francia rispetto alla concorrenza internazionale in termini di numero di imprese;
- far emergere le eccellenze francesi della *cybersecurity* affidandosi alle maggiori start-up del settore, e in particolare a quelle appartenenti a French Tech 120;
- diffondere una vera cultura della *cybersecurity* nelle aziende;
- stimolare la ricerca francese nell'innovazione informatica e industriale (aumento del 20% dei brevetti).

La strategia di *cybersecurity* è stata costruita in piena collaborazione tra le amministrazioni competenti in materia cibernetica e gli attori dell'ecosistema (produttori, enti di ricerca, comunità, ecc.). È suddivisa in **cinque aree**:

a. sviluppo di soluzioni di sicurezza informatica sovrane e innovative;
b. rafforzamento dei legami e delle sinergie tra gli attori del settore;
c. sostegno alla domanda (individui, aziende, comunità e Stato), in particolare sensibilizzando e promuovendo offerte nazionali;
d. formazione dei più giovani e dei professionisti nel settore della sicurezza informatica, che attualmente scontano un forte squilibrio;
e. sostegno all'equità.

In particolare, sono stati previsti una serie di bandi per l'assegnazione di risorse pubbliche. Il primo di questi, in scadenza il 16 giugno 2021, prevede 20 milioni di sussidi pubblici (per un totale di 40 milioni) ed ha come titolo "*Sécuriser les territoires*" (Mettere in sicurezza i territori)[7].

Nell'ambito della nuova strategia il Governo ha inteso rafforzare la *cybersecurity* per le **strutture sanitarie e medico-sociali** (*établissements sanitaires et médico-sociaux*) e in tal senso il *Ségur de la Santé*[8] ha deciso lo stanziamento di **350 milioni di euro** specificamente dedicati al rafforzamento della sicurezza informatica in questi settori. L'importanza della sicurezza informatica sarà inoltre evidenziata in tutti i corsi di formazione per gli attori sanitari per sviluppare pratiche di "igiene digitale" (*hygiène numérique*). Entro il 2021, 135 gruppi ospedalieri francesi saranno inclusi nell'elenco degli operatori di servizi essenziali, il che implica regole di sicurezza informatica più severe e il controllo dell'ANSSI sul corretto rispetto di tali regole.

Infine, il 18 febbraio 2021, il Presidente della Repubblica francese Emmanuel Macron, a seguito di uno studio di fattibilità richiesto nel 2019, ha confermato la creazione di un *cybercampus* nel quartiere de *La Défense*, dedicato alle questioni digitali, con particolare riguardo alla sicurezza informatica, e che porterà piccole, medie e grandi imprese a riunirsi in un unico luogo per promuovere gli scambi in questi settori.

Germania

1. Strategia nazionale ed atti normativi in materia di cybersicurezza

I progressi compiuti dalla Germania in campo informatico e nell'*high tech* hanno fatto sì che il paese – leader europeo nel settore ICT e quarto al mondo – si confrontasse con le sfide della sicurezza informatica e delle telecomunicazioni in anticipo rispetto ad altri stati europei. Una delle prime iniziative intraprese dal Governo federale è stata infatti l'istituzione dell'**Ufficio federale per la sicurezza informatica** (*Bundesamt für Sicherheit in der Informationstechnik* - BSI), che ha ufficialmente iniziato la sua attività il 1° gennaio 1991. Ai sensi del § 1 della vigente legge che lo regolamenta (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, *BSI-Gesetz* – BSIG del 14 agosto 2009), recentemente modificata dalla *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (2. ITSiG)* del 18 maggio 2021 (Seconda legge per migliorare la sicurezza dei sistemi di informazione digitale), il BSI è competente per la sicurezza informatica a livello nazionale e costituisce un'autorità centrale che opera nell'ambito della sfera di competenza del Ministero federale dell'interno, dei lavori pubblici e della patria. L'Ufficio federale per la sicurezza informatica, i cui poteri sono stati notevolmente ampliati con le modifiche alla legge originaria approvate il 17 luglio 2015, assolve inoltre specifiche funzioni a favore dei ministeri federali sulla base di prove scientifiche e tecniche. Le aree di competenza di questa agenzia federale, con sede a Bonn e nella quale lavorano attualmente circa 570 dipendenti, comprendono la protezione delle reti informatiche del Governo federale, la sicurezza delle applicazioni e installazioni informatiche, la verifica e certificazione dei *software* e dei servizi, e, più recentemente, l'allerta da infezioni da *malware*.

La **strategia nazionale sulla cybersicurezza e sulla sicurezza informatica** è stata inizialmente inserita in un contesto di innovazione più ampio che copre tutti i settori strategici ad alta tecnologia. Tale strategia, denominata "***High-Tech Strategie 2020***", è

[7] Sul sito del Ministero dell'Economia, della Finanze e del Rilancio sono consultabili i dettagli di questo e degli altri bandi che verranno pubblicati.

[8] Si tratta di una consultazione delle parti interessate nel sistema sanitario francese che si è svolta dal 25 maggio al 10 luglio 2020.

contenuta in una serie di documenti redatti a partire dal 2006 e aggiornata con cadenza quadriennale seguendo le raccomandazioni di un panel di esperti che dal 2006 al 2013 ha ospitato dapprima solo rappresentanti della ricerca e dell'industria, e, a partire dal 2014, anche membri della società civile.

Negli ultimi piani strategici sono state individuate come aree chiave:

- la ***cybersecurity***: le sfide in quest'area riguardano tutte le azioni criminali che possono violare privacy o segreti industriali, mirando all'accesso e all'intercettazione non autorizzata dei dati. Il Governo federale ha riconosciuto priorità alla ricerca sull'informatica forense e la criminologia. L'implementazione del programma è descritta nella *Cyber-Sicherheitsstrategie für Deutschland*, adottata nel febbraio 2011 e poi aggiornata nel 2016. È stata predisposta una **bozza di nuova strategia** da approvare entro il 2021*: Entwurf der Cybersicherheitsstrategie für Deutschland 2021;*
- l'***IT Sicherheit***: ha come obiettivo pricipale l'affidabilità e la sicurezza delle reti. Il Governo federale supporta la ricerca nell'IT security con due programmi di finanziamento: "*Selbstbestimmt und sicher in der digitalen Welt 2015-2020*"[9] per la ricerca accademica (attuato dal Ministero Federale dell'Istruzione e della Ricerca Scientifica), e "*IT Sicherheit in der Industrie*" per le piccole e medie imprese, al fine di migliorare i loro livelli di sicurezza;
- le **identità sicure**: la sicurezza delle identità rappresenta un elemento di particolare interesse per il Governo federale. Esse sono alla base della privacy e del commercio elettronico. Il Governo federale continua a sostenere la ricerca nella creazione di nuovi approcci interdisciplinari con il forum "*Privacy - Self-Determined Living in the Digital World*".

E' stata inoltre recentemente approvata la **Strategia High-Tech 2025** (*Research and innovation that benefit the people. The High-Tech Strategy 2025*) che si pone l'obiettivo di far diventare la Germania un leader mondiale nel settore dell'innovazione. L'obiettivo è quello di tradurre rapidamente le buone idee in prodotti e servizi innovativi. Cospicui finanziamenti sono stanziati per la ricerca e l'innovazione nei settori della mobilità, dell'energia, della salute, della sicurezza e dell'economia. La strategia ha **tre pilastri principali**: a) affrontare le principali sfide sociali; b) rafforzare le competenze attraverso l'istruzione e la formazione; c) sviluppare una cultura aperta e innovativa. Uno dei suoi progetti di punta è l'Iniziativa *Spitzencluster (cluster di eccellenza)* che collega imprese, istituti di ricerca, università e altri attori locali rilevanti per creare sinergie a fini di ricerca e innovazione.

Un primo concreto esito dell'**Agenda digitale** (*Digitale Agenda 2014-2017*), adottata dal Governo federale nel 2014, è rappresentato dalla già citata **Legge per aumentare la sicurezza dei sistemi informatici** (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, IT-Sicherheitsgesetz*) del 17 luglio 2015, con la quale sono state introdotte nuove disposizioni volte a garantire la sicurezza dei sistemi informatici in alcuni settori chiave come quello energetico, alimentare, idrico, sanitario, finanziario e dei trasporti (c.d. **infrastrutture critiche**, *Kritische Infrastrukturen* – **KRITIS**). L'obiettivo della legge è anche quello di migliorare la sicurezza informatica nelle aziende e nell'amministrazione federale, nonché offrire ai cittadini una migliore protezione online. Per la realizzazione di questi scopi sono state estese le funzioni e le competenze del già citato Ufficio federale per la sicurezza informatica che, ai sensi del § 8b *BSI-Gesetz,* svolge anche la funzione di **Ufficio di registrazione centrale per gli**

[9] Sul sito del Ministero è disponibile anche la traduzione inglese del programma.

operatori delle infrastrutture critiche nelle questioni riguardanti la sicurezza informatica (*Zentrale Meldestelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen*).

L'*IT-Sicherheitsgesetz* del 2015 prevede a carico degli operatori delle infrastrutture strategiche l'obbligo di adottare, entro limiti di costo ragionevoli, provvedimenti specifici in materia di cybersicurezza in linea con il costante progresso tecnologico, ossia quelle misure organizzative e tecniche necessarie ad evitare inconvenienti tecnici inerenti alla disponibilità, integrità, autenticità e riservatezza dei loro sistemi informatici. Alcune norme specifiche, applicabili al settore delle telecomunicazioni, riguardano il monitoraggio e l'obbligo, per le imprese di questo settore, di avvisare i propri clienti se constatano un uso improprio della connessione mostrando le possibili soluzioni, mentre altre disposizioni *ad hoc* si applicano alle società di energia nucleare che devono rispettare uno *standard* di sicurezza più elevato. Specifiche previsioni riguardano i fornitori di servizi audiovisivi, i quali sono tenuti ad adottare misure volte ad impedire l'accesso non autorizzato ai sistemi utilizzati per la fornitura del servizio e il trattamento illecito dei dati personali.

Gli operatori delle infrastrutture critiche devono inviare ogni due anni all'Ufficio federale per la sicurezza informatica una valutazione recante le informazioni relative alle misure concretamente adottate e ai *bugs* registrati nei loro sistemi informatici. È inoltre previsto l'obbligo di notificare allo stesso Ufficio gravi episodi di *hacking* ed eventuali inadempienze in fatto di sicurezza, nonché il nominativo del referente aziendale in materia di sicurezza informatica. Il mancato rispetto degli obblighi previsto dalla legge è punito con una sanzione pecuniaria fino a 100 mila euro per le violazioni più gravi (§ 14 *BSI-Gesetz*).

La già citata **Seconda legge per migliorare la sicurezza dei sistemi di informazione digitale** (*Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*), del 18 maggio 2021, rafforza inoltre i poteri del BSI nello svolgimento delle seguenti funzioni:

- **Rilevamento e difesa**: il BSI dispone ora di nuove competenze nel rilevamento delle possibili falle nella sicurezza e nella difesa dagli attacchi informatici. In qualità di centro di competenza centrale per la sicurezza delle informazioni, il BSI può progettare una digitalizzazione sicura e, tra l'altro, **stabilire standard minimi vincolanti per le autorità federali e controllarli in modo più efficace**;
- **Sicurezza informatica nelle reti cellulari**: la legge del maggio 2021 introduce nel testo originario una disposizione che vieta l'uso di componenti critici per proteggere l'ordine pubblico o la sicurezza in Germania. Gli operatori di rete devono inoltre soddisfare elevati e specifici requisiti di sicurezza e i componenti critici devono essere certificati. La legge garantisce, inoltre, la sicurezza delle informazioni nelle reti mobili 5G;
- **Tutela dei consumatori**: il BSI sarà il centro di consulenza indipendente e neutrale per i consumatori su questioni di sicurezza informatica a livello federale. La protezione dei consumatori è quindi ora un compito del BSI. L'introduzione di un'etichetta di sicurezza informatica uniforme per i cittadini dovrebbe inoltre rendere la sicurezza informatica più trasparente e chiaramente riconoscibile in futuro;
- **Sicurezza per le aziende**: il perimetro di definizione delle infrastrutture critiche si allarga al settore dello smaltimento dei rifiuti urbani. Inoltre, altre aziende di particolare interesse pubblico (ad esempio, produttori di armamenti o aziende di particolare rilevanza economica) dovranno attuare determinate misure di

sicurezza informatica e saranno incluse nello scambio di informazioni di fiducia con il BSI.

Come previsto dal § 10 *BSI-Gesetz*, il 3 maggio 2016, in attuazione della *IT-Sicherheitsgesetz*, è entrato in vigore un primo gruppo di disposizioni del **Regolamento sulle infrastrutture critiche** (*Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, BSI-Kritisverordnung - BSI-KritisV*, del 22 aprile 2016), gruppo applicabile ai settori dell'energia, dell'informatica, delle telecomunicazioni, dell'acqua e dell'alimentazione. Le disposizioni relative ai settori finanziario, assicurativo, sanitario e dei trasporti sono invece entrate in vigore oltre un anno più tardi, il 30 giugno 2017, a seguito di alcune modifiche integrative al regolamento del 2016 (*Erste Verordnung zur Änderung der BSI-Kritisverordnung*, del 21 giugno 2017). Si segnala, infine, che è in fase di discussione una bozza di *Zweite Verordnung zur Änderung der BSI-Kritisverordnung*, pubblicata dal Ministero Federale dell'Interno il 26 aprile 2021.

2. Organismi ed enti federali preposti alla cybersicurezza

Elemento centrale della citata strategia di cybersicurezza è stata l'istituzione del **Centro nazionale di difesa cibernetica** (*Nationale Cyber-Abwehrzentrum - Cyber-AZ*), una struttura di cooperazione di autorità e organismi di sicurezza che operano a livello federale per la difesa da attacchi informatici. Il *Cyber-Az*, istituito in base a una decisione del Governo federale del 23 febbraio 2011, ha sede a Bonn presso l'Ufficio federale per la sicurezza informatica. I principali compiti del Centro sono la prevenzione, l'informazione e l'allerta precoce contro i c.d. attacchi informatici (*Cyber-Angriffe*) diretti contro uno o più sistemi informatici allo scopo di comprometterne la sicurezza.

Per quanto riguarda più specificamente il settore della difesa, che solo nei primi tre mesi del 2017 ha subito 284 mila attacchi informatici, tutte le funzioni relative alla cybersicurezza sono state accentrate in una **nuova struttura interforze** con quartier generale a Bonn, l'**Unità di cyberdifesa nazionale** (*Kommando Cyber- und Informationsraum - KdoCIR*) inaugurata alla presenza dell'allora Ministro federale della difesa Ursula von der Leyen ed entrata in funzione il 5 aprile 2017 per sovrintendere alle operazioni cibernetiche e coordinare l'infrastruttura IT, le comunicazioni militari, operative e i servizi di geolocalizzazione. Il *KdoCIR* rappresenta quindi l'equivalente del *Cyber-AZ* – creato solo per scopi civili – sul piano militare. L'Unità, che dispone di un *team* di 13.500 effettivi su tutto il territorio della Germania sotto il comando del generale Ludwig Leinhos, raggiungerà la piena operatività nel 2021. La Germania ha quindi ideato, come è stato definito dalla stampa, un corpo di *cyber marines* in grado di fronteggiare la difficile sfida della cybersicurezza a livello globale e che potrebbe rappresentare un primo passo verso la costituzione di una specie di corpo di armata unico per la cyberdifesa dell'Unione europea.

Successivamente, il 14 settembre 2017, è stata inaugurata a Monaco di Baviera una **nuova Agenzia per la cybersicurezza** (Ufficio centrale per l'informatica nel settore della sicurezza, *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* – **ZITiS***)* come parte di un tentativo centralizzato per affrontare la criminalità informatica e lo spionaggio digitale mediante la sorveglianza delle telecomunicazioni di massa, la crittografia dei dati e la raccolta delle informazioni. Dal punto di vista giuridico, lo ZIYiS è stato istituito come ente federale senza capacità giuridica nella sfera di competenza del Ministero federale dell'interno con un decreto ministeriale (*Erlass*), emanato il 6 aprile 2017 dall'allora Ministro federale dell'interno De Maizière.

Lo ZITiS, come ha dichiarato lo stesso Ministro federale dell'interno, rappresenta un investimento di grande importanza, destinato a diventare una risorsa tecnologica a

servizio degli altri servizi di sicurezza della Germania. I compiti della nuova Agenzia includono anche la "scienza forense digitale" per poter sviluppare nuovi metodi finalizzati alla raccolta di prove provenienti da internet. Lo ZITiS, il cui organico iniziale è di 120 unità per un investimento iniziale di 10 milioni di euro, ricerca ed elabora strategie di sorveglianza delle telecomunicazioni per conto di altre agenzie.

Da ultimo, il 6 settembre 2018 il Governo federale ha approvato la creazione di un'**Agenzia per per l'innovazione nella cybersicurezza** (*Agentur für Innovation in der Cybersicherheit*) investendo 200 milioni di euro in un programma di durata quadriennale. La nuova agenzia governativa, creata nel 2020, è guidata congiuntamente dal Ministero Federale della Difesa e dal Ministero Federale dell'Interno con l'obiettivo di proteggere e difendere lo Stato dalle minacce del futuro, *in primis* dai *cyber* attacchi. Il modello per la creazione di questa nuova organizzazione governativa è stata la *Darpa* del Pentagono USA (*Defense Advanced Research Projects Agency*). Lo scopo dei funzionari del Ministero Federale della Difesa che lavorano al progetto è quello di rafforzare la rete di sicurezza informatica del paese con l'acquisizione di tecnologie adeguate, garantendo la sicurezza dei dati sensibili e lo sviluppo di contromisure per difendere la Germania e i paesi alleati della Nato dai sofisticati attacchi di *hacker* (o *cracker*) che si sono moltiplicati nell'ultimo triennio.

Per completare il quadro delle istituzioni impegnate a livello federale nel realizzare gli obiettivi della strategia relativa alla cybersicurezza, si segnala infine la **risposta scritta del Governo federale** (stampato BT n. 19/2645 dell'11 giugno 2018) ad un'interrogazione presentata dai deputati del gruppo parlamentare liberale in merito all'esistenza di dipartimenti, nella sfera di competenza di vari Ministeri federali, che si occupano di cyberdifesa e di contro-attacchi informatici.

Regno Unito

Il tema della sicurezza delle **infrastrutture di interesse nazionale** (*critical national infrastructures* – CNI) e della loro esposizione al rischio di attacchi cibernetici è stato oggetto, negli ultimi anni, di specifiche iniziative del Governo e del Parlamento del Regno Unito. L'impatto dell'evoluzione tecnologica e il pericolo di *cyber-attacks*, con effetti potenzialmente dirompenti sull'organizzazione sociale ed economica nazionale, sono stati annoverati dal Governo tra le maggiori sfide poste al Paese al momento di sottoporre a verifica, nel 2018, lo stato di attuazione della strategia per la sicurezza e la difesa adottata nel 2015[10]. Tali iniziative, d'altra parte, si sono delineate in un quadro normativo e istituzionale assai articolato.

In tema è di riferimento generale la legislazione applicabile ai reati a carattere informatico, compresa l'intrusione abusiva in sistemi informatici; essa forma un *corpus* normativo stratificato di cui fanno parte, tra le altre, le previsioni in materia di *hacking* (*Computer Misuse Act 1990*), di furto di identità (*Fraud Act 2006*), di sicurezza riferita rispettivamente alle telecomunicazioni (*Communications Act 2003*) e ai dati personali (materia ora disciplinata dal Regolamento UE 2016/679 e dal *Data Protection Act 2018* quale disciplina nazionale di adattamento); nonché, per gli aspetti rilevanti, dalla disciplina sul contrasto delle attività di stampo terroristico (*Terrorism Act 2000*) e sulla intercettazione delle comunicazioni (*Investigatory Powers Act 2016*).

In relazione più specifica al tema della cibersicurezza, il Governo ha dato attuazione, con le *Network and Information System Regulations 2018*[11], alla recente disciplina euro-

[10] *National Security Capability Review* (marzo 2018), concernente il secondo anno di implementazione della *National Security Strategy 2015* e della *Strategic Defence and security Review 2015*.

[11] S.I. 2018 n. 506.

unitaria in materia, prevedendo misure di sicurezza[12] per le infrastrutture nazionali in tredici ambiti prioritari[13].

La portata innovativa delle *regulations* ben si comprende ove si consideri che la disciplina delle infrastrutture di interesse nazionale è stata prima applicata da *authorities* di regolazione, competenti a vigilare sull'assetto della concorrenza dei mercati di riferimento oppure anche su profili inerenti alla sicurezza (*economic* o *security regulators*), assolvendo in taluni casi ad entrambi i compiti (è il caso, dal 2011, di Ofcom, autorità di regolazione delle telecomunicazioni); per converso, l'introduzione del principio della **resilienza** rispetto ai rischi di *cyber-attacks* comporta ora il complessivo e uniforme incremento dei livelli di sicurezza nel settore dei servizi essenziali, in prospettiva soprattutto della continuità della loro erogazione.

Tale obiettivo è perseguito dalle *regulations* attraverso l'obbligo posto sugli operatori (incluse le pubbliche amministrazioni) di implementare misure di sicurezza "appropriate e proporzionate"; l'istituzione di *competent authorities*, ovvero di autorità di regolazione e controllo, in ciascun settore al quale si applica la disciplina, al fine di assicurarvi il rispetto delle prescrizioni; l'individuazione di un unitario "punto di contatto" nell'ambito del Governo nazionale, che sia di riferimento per gli altri Stati membri dell'Unione Europea, e la creazione di un *team* abilitato alla gestione degli incidenti (le cui funzioni, assieme a quelle del "*single point of contact*", sono assolte dal *National Cyber Security Centre* su cui *infra*).

Il raggio applicativo delle ***regulations*** si estende ai settori delle risorse idriche, della sanità, dei trasporti, delle telecomunicazioni, mentre ne è escluso l'ambito finanziario e bancario (pur contemplato dalla direttiva), nel presupposto esso sia già oggetto di normative specifiche. Gli operatori dei settori implicati (i cui servizi sono considerati "essenziali", ai fini della normativa, in relazione a soglie numeriche riferite alla platea dei rispettivi utenti), sono tenuti a conformarsi alle linee-guida predisposte dalle competenti autorità di regolazione (le quali a loro volta adottano a base della propria attività le regole di "buona pratica" stabilite dal *National Cyber Security Centre*). Le *regulations*, infine, fanno obbligo agli operatori di denunciare tempestivamente, entro 72 ore, gli incidenti il cui impatto superi soglie predeterminate dalle *authorities* di riferimento; e prevedono, per la violazione delle prescrizioni in materia di cyber-sicurezza, **sanzioni pecuniarie** di ammontare fino a 17 milioni di sterline.

Significative innovazioni in materia di cyber-sicurezza, peraltro, si correlano all'adozione, nel 2016, del **piano strategico nazionale** quinquennale ad essa specificamente dedicato (*National Cyber Security Strategy 2016-2021* - NCSS[14], dotata di uno stanziamento di 1,9 miliardi di sterline).

In questa occasione il Governo ha mutato l'impostazione accolta nel piano strategico riferito al quinquennio precedente[15], che assegnava ampio spazio all'iniziativa degli operatori privati e al mercato per la diffusione e l'implementazione di elevati standard di sicurezza nel settore sia privato che pubblico; constatando i limitati vantaggi di un simile

[12] Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[13] I tredici settori delle *critical national infrastructures* individuati dal Governo sono quelli della chimica, dell'energia nucleare civile, delle comunicazioni, della difesa, dei servizi di protezione civile, dell'energia, della finanza, delle risorse alimentari, dell'amministrazione pubblica, nonché la sanità, il settore aerospaziale, i trasporti e le risorse idriche.

[14] *National Cyber Security Strategy 2016-2021*.

[15] Si tratta della prima *National Cyber Security Strategy* riferita al periodo 2011-2016, adottata nel 2010 e finanziata con uno stanziamento di 860 milioni di sterline.

approccio esso ha infatti riconosciuto, per il perseguimento del medesimo obiettivo, il ruolo dei poteri pubblici e la maggiore incisività del loro intervento[16].

In particolare, si è provveduto ad istituire un organismo tecnico *ad hoc*, il ***National Cyber Security Centre*** (NCSC)[17], preposto alla gestione degli incidenti di rilievo nazionale nel campo della cibersicurezza e all'assistenza tecnica diretta ai dipartimenti governativi, alle amministrazione pubbliche e alle imprese attraverso attività di analisi e di individuazione delle minacce, di consulenza, di promozione dell'innovazione e delle competenze professionali in materia[18]. Nell'espletamento dei suoi compiti il NCSC si inserisce nella rete di collaborazione tra gli organismi le cui competenze riguardano la sicurezza dello Stato (*Government Communications Headquarter* – GCHQ[19]) e la protezione delle infrastrutture di interesse nazionale (CPNI[20]).

Il piano strategico vigente condensa i propri obiettivi avvalendosi tre fondamentali parole-chiave: *Defend*, *Deter*, *Develop*. Ovvero si fa riferimento (*Defend*) alla resilienza delle reti di comunicazione nel settore pubblico e in quello privato ed imprenditoriale rispetto agli attacchi esterni, e in particolare lo schema (denominato *Active Cyber Defence*) che fa leva sull'adozione, in modo appropriato e "proattivo", di misure di sicurezza idonee a rafforzare i livelli di tutela. Viene altresì postulata la complessiva capacità del sistema a dispiegare un'azione di deterrenza (*Deter*) rispetto a simili minacce, elevando i costi necessari a metterle in atto e riducendo i benefici che da ciò possono trarsi, anche attraverso l'inasprimento delle sanzioni e il dispiegamento di misure diplomatiche, politiche, economiche. Infine, si persegue in ambito nazionale lo sviluppo (*Develop*) delle competenze e capacità professionali e tecnologiche necessarie alla tutela del Paese dai rischi suddetti.

Nel piano strategico, infine, è fatto riferimento all'uscita del Regno Unito dall'Unione Europea, affermandosi al riguardo la necessità della continuazione degli accordi di **cooperazione internazionale** in questo ambito – specie con la *European Union Agency for Network and Information Security* (ENISA) -, stante l'evidente carattere transnazionale dei fenomeni considerati.

Sul versante parlamentare, deve segnalarsi l'**indagine** condotta dalla commissione bicamerale competente (*Joint Committee on National Security Strategy*) sull'attuazione del piano strategico da ultimo richiamato.

La commissione ha espresso, anche sulla base delle risultanze acquisite attraverso un ciclo di audizioni, alcune riserve circa la complessiva adeguatezza delle misure previste rispetto alla gravità dei rischi a cui sono esposte le infrastrutture vitali del Paese, dovendosi queste considerare come i possibili "bersagli naturali" di attacchi perpetrati attraverso le reti di telecomunicazione da gruppi criminali o da Stati stranieri al fine di interferire con il loro regolare funzionamento, o di violare segreti industriali e diritti di privativa, oppure di compiere atti di spionaggio. La commissione ha pertanto evidenziato, nella relazione pubblicata nel novembre 2018[21], una serie di aspetti per i quali ha

[16] "Only Government can draw on the intelligence and other assets required to defend the country from the most threats. Only Government can drive cooperation across the public and private sectors and ensure information is shared between two. Government has a leading role, in consultation with industry, in defining what good cyber security looks like and it is implemented": *National Cyber Security Strategy 2016-2021*, p. 27.

[17] Del NCSC può consultarsi la *Annual Review 2020*.

[18] Un bilancio dell'attività finora svolta dal NCSC v. la relazione del Cabinet Office, *National Cyber Security Strategy 2016-2021 – Progress report*.

[19] Si segnala al riguardo che il NCSC ha assorbito il CESG, precedentemente incardinato nel GCHQ come sua articolazione deputata alla *information security*.

[20] *Center for Protection of National Infrastructure*.

[21] House of Lords – House of Commons, Joint Committee on National Security Strategy, *Cyber security of the UK's Critical national Infrastructure* (Third Report of Session 2017-2019).

segnalato al Governo l'esigenza di assicurare maggiori livelli di **resilienza** delle infrastrutture suddette, nella consapevolezza che sia impossibile garantirne la sicurezza assoluta e che la capacità di rispondere ad insidie ripetute e costanti, da parte di soggetti statali e non statali, rappresenti ormai il parametro della normalità[22].

D'altra parte il grado di interconnessione e di interdipendenza instauratosi tra le diverse infrastrutture, a giudizio della commissione, rende ormai inadeguata la designazione di ciascuna di queste come prioritaria, poiché gli incidenti che potrebbero colpirle avrebbero inevitabilmente ricadute sugli operatori di altri settori. Pertanto, mentre si auspica l'adozione di un approccio "sistemico" in occasione della redazione del prossimo piano strategico in materia, è raccomandata la preposizione di un Ministro membro del *Cabinet Office* all'attività di coordinamento delle attuali misure di *cyber–resilience* concernenti i singoli ambiti infrastrutturali.

Inoltre, come già evidenziato in una precedente relazione del luglio 2018[23], il Regno Unito registra la perdurante carenza di **profili professionali** specialistici nei maggiori settori infrastrutturali; il tema è stato preso in specifico esame dalla commissione bicamerale, che proprio nel "cambiamento culturale" ha individuato la condizione affinché possa aversi un costante miglioramento al passo con l'evoluzione tecnologica.

La raccomandazione della commissione bicamerale generalmente rivolta ad un'espansione dell'intervento dello Stato in un ambito di tale complessità (e in cui, a suo avviso, si è registrato anche un "fallimento del mercato" le cui cause il Governo ha finora mancato di valutare adeguatamente), è stata seguita dall'annuncio (l'11 maggio 2019)di un progetto di legge dedicato al particolare profilo della cibersicurezza nell'ambito dell'"Internet delle cose" (***Internet of things*** – "**Iot"**), di rilevante impatto sociale ove si consideri la pervasività delle correlate applicazioni tecnologiche, di crescente diffusione anche in ambito domestico[24].

Le linee fondamentali della disciplina, finalizzata ad introdurre, tra l'altro, requisiti minimi obbligatori di sicurezza incorporati nei dispositivi tecnologici fin dalla loro fabbricazione, è stata oggetto di una consultazione pubblica[25] promossa dal *Department for Digital, Culture, Media and Sport* nel quadro dell'iniziativa denominata *Secure by design*[26], concretizzatasi in una serie di documenti programmatici e di codici di condotta concernenti gli standard di sicurezza e la tutela dei consumatori in questo settore.

Nel mese di aprile 2021 il Governo britannico ha annunciato l'adozione di ulteriori **misure legislative**, dedicate in particolare ai dispositivi tecnologici ricompresi nella categoria anzidetta dell'*Internet of things*. Il presupposto da cui muove il Governo è che l'uso intensivo di tali dispositivi generalmente effettuato durante la pandemia abbia messo in evidenza la loro vulnerabilità rispetto ad interferenze e ad accessi abusivi ai dati personali degli utilizzatori, e che a fronte di questo rischio – come emerso da uno studio della *University College London*[27] - la maggior parte dei dispositivi di telecomunicazione non è corredata da informazioni relative al loro livello di sicurezza e di protezione.

Inoltre, il legislatore ha affrontato il tema della **sicurezza delle reti di telecomunicazioni** in relazione alla sicurezza nazionale, specie in considerazione

[22] V. il documento citato alla nota precedente, p. 12.
[23] House of Lords – House of Commons, Joint Committee on National Security Strategy, *Cyber Security Skills and the UK's Critical National Infrastructure* (Second Report of Session 2017-2019). Sul tema dello *skill gap* in questo ambito vedasi la replica del Governo alla relazione parlamentare, del 13 novembre 2018.
[24] *Plans announced to introduce new laws for internet connected devices* (press release, 1 May 2019).
[25] *Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security*. La replica del Governo alle posizioni espresse nel corso della consultazione è stata pubblicata nel dicembre 2020: *Consumers Attitudes Towards Iot Security*.
[26] *Secure by Design*.
[27] *Networked World: Risks and Opportunities in the Internet of Things* (2018).

dell'evoluzione tecnologica delle infrastrutture e della programmata applicazione dello standard "5G", adottando misure legislative (contenute nel ***Telecommunications Security Bill*** attualmente all'esame parlamentare[28]) che in modifica del *Communication Act* del 2003 prescrivono particolari **obblighi di sicurezza** ai gestori delle reti e ai fornitori di servizi di telecomunicazione. I doveri e le responsabilità di questi soggetti sono infatti accresciuti dalle previsioni legislative in relazione all'adozione di requisiti di sicurezza la cui definizione può avere luogo anche in conseguenza di direttive o di codici di condotta emanati dal Ministro competente di concerto con l'autorità di regolazione del settore (*Ofcom*). Ai *providers* di servizi di telecomunicazione accessibili al pubblico, in particolare, è fatto obbligo di adottare le misure "appropriate e proporzionali" allo scopo di individuare, prevenire e mitigare i rischi per la sicurezza, questi ultimi definiti come "qualsiasi fattore possa compromettere la disponibilità, l'efficienza, la funzionalità della rete o del servizio, o la riservatezza del segnale trasmesso" attraverso tali mezzi. I fornitori devono pertanto effettuare una valutazione dei rischi e configurare le reti o i servizi in modo da minimizzarli[29].

Nel quadro delle medesime finalità (e successivamente alle polemiche insorte con riguardo alla crescente penetrazione di soggetti industriali stranieri in settori "sensibili") il legislatore ha recentemente approvato, il 5 maggio 2021, il *National Security and Investment Act 2021*, che abilita il Governo ad esercitare poteri di controllo e di intervento con riguardo alla conclusione di accordi commerciali ritenuti rilevanti per la sicurezza nazionale.

[28] *Telecommunication Security Bill*, presentato il 26 maggio 2021 e attualmente all'esame in seconda lettura presso la Camera dei Lord.
[29] In tema v. la nota di documentazione della House of Commons Library, *Telecommunications Security Bill 2019-21*, n. 9063, 21 May 2021.