CAMERA DEI DEPUTATI N. **3161**

DISEGNO DI LEGGE

PRESENTATO DAL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

(**DRAGHI**)

Conversione in legge del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

Presentato il 14 giugno 2021

RELAZIONE

La digitalizzazione della società offre, e offrirà sempre di più nei prossimi tempi, grandi vantaggi, creando al contempo, tuttavia, nuove interdipendenze tra filiere produttive, amministrazioni e cittadini, dovute alla complessità delle interazioni tra i sistemi informatici. Tutto ciò genera nuovi rischi come quello di introdurre vulnerabilità strutturali all'interno di servizi e funzioni essenziali dello Stato, che potrebbero essere usate per finalità criminali o per gli interessi di altri attori statuali, come ad esempio nelle reti 5G o nei sistemi di intelligenza artificiale (IA). Inoltre, l'attuale crisi pandemica ha reso ancora più evidente come una società, che basi il suo futuro su un processo massiccio di trasformazione digitale, soffra un'accresciuta esposizione ad attacchi cyber. Ciò avviene anche a causa delle modalità di sviluppo dei prodotti ICT, per lungo tempo realizzati con il primario obiettivo di incrementarne l'efficacia e la facilità d'uso per l'utente, nonché di ridurne i costi, spesso ponendo in secondo piano, e in alcuni casi tralasciando completamente, gli aspetti di sicurezza.

Da questo scenario deriva l'esigenza di approcciare tale problematica secondo una dimensione olistica, in cui:

- vengano definite adeguate strategie di cybersicurezza, intesa quale insieme di attività necessarie per proteggere e assicurare la disponibilità, la confidenzialità e l'integrità di reti, sistemi informativi, servizi informatici e comunicazioni elettroniche dalle minacce informatiche, garantendone altresì la resilienza. Tali strategie dovranno essere volte a pianificare, coordinare e attuare misure tese a rendere il Paese più sicuro e resiliente anche nel dominio digitale, rafforzando, al contempo, la fiducia dei cittadini nella possibilità di sfruttarne i relativi vantaggi competitivi, nella piena tutela dei diritti e delle libertà fondamentali. In questo contesto, è determinante sviluppare capacità avanzate (che includano processi tecnologici come la certificazione) tese ad assicurare l'intero ciclo della resilienza (prevenzione, scoperta, attività di allertamento di attacchi, mitigazione e recupero), così da poter gestire i rischi legati ad attacchi cibernetici endemici lanciati da attori diversificati;
- vengano poste la sicurezza e la resilienza cibernetiche, divenute sempre più strettamente legate alla più complessiva dimensione della sicurezza nazionale, a fondamento del processo di digitalizzazione del Paese, quale prerequisito indispensabile della trasformazione digitale, anche nell'ottica dell'innovazione industriale e dell'autonomia strategica nella cybersicurezza favorendo e coordinando lo sviluppo tecnologico e scientifico nazionale nel settore;
- si punti ad accrescere, attraverso la promozione della cultura della cybersicurezza, la consapevolezza del settore pubblico e privato e della società civile sui rischi e le minacce cyber. Tutte queste realtà devono, infatti, percepire il proprio ruolo quale parte attiva e responsabile all'interno del Sistema Paese, attuando comportamenti sicuri e virtuosi nello spazio cibernetico. Tali comportamenti, infatti, costituiscono fattori abilitanti per lo sviluppo e la crescita dell'economia e dell'industria nazionale, al fine di accrescere la competitività del Sistema Paese a livello globale;
- vengano poste solide basi formative in ambito cyber con diversi livelli di specializzazione in cybersicurezza (scuola superiore professionale, corsi universitari, master, dottorati), mirando a stimolare la creazione di una solida forza lavoro nazionale, composta da esperti e giovani

talenti in possesso delle capacità e delle competenze necessarie per poter essere applicate a beneficio del Sistema Italia;

- si persegua un'effettiva capacità di mantenere relazioni bilaterali e multilaterali, nonché di partecipare attivamente ai processi di definizione di politiche, norme e standard internazionali in materia, per favorire lo scambio di informazioni e di conoscenze, promuovere l'internazionalizzazione delle imprese attive nel settore e rafforzare il posizionamento del Paese.

Il perseguimento degli obiettivi descritti necessita, come è già avvenuto anche in altri Paesi (si pensi alla Francia, alla Germania o al Regno Unito), della costituzione di un'agenzia nazionale di cybersicurezza, a cui attribuire direttamente la responsabilità delle attività descritte, concentrando in essa le funzioni specialistiche in materia – tese ad innalzare i livelli di resilienza nel dominio digitale – ad esclusione di quelle attinenti alla *cyber-intelligence* (di competenza degli organismi di informazione per la sicurezza), alla *cyber-defense* (intesa come difesa e sicurezza militare dello Stato, di competenza del Ministero della difesa) e alla prevenzione e repressione dei reati (di competenza delle Forze di polizia). A ciò deve accompagnarsi il più ampio ruolo di coordinamento e stretta sinergia con tutte le altre amministrazioni coinvolte *ratione materiae* (*intelligence*, Difesa, Forze di polizia, strutture preposte alla protezione fisica delle infrastrutture critiche, Ministeri degli affari esteri e della cooperazione internazionale, dello sviluppo economico, dell'innovazione tecnologica e della transizione digitale, dell'università e della ricerca, etc.), in modo da assicurare iniziative coerenti, efficientamento della spesa, capacità di fornire un chiaro e aggiornato quadro situazionale all'Autorità politica, nonché un'interfaccia unica a livello nazionale, europeo e internazionale, assicurando le relative posture nazionali unitarie.

In tale ottica, si pone dunque l'esigenza di ridefinire la complessiva Architettura nazionale cyber, che a partire dalla legge 7 agosto 2012, n. 133, ha visto via via l'attribuzione al Comparto *intelligence* e, in particolare, al Dipartimento delle informazioni per la sicurezza, di compiti e funzioni pienamente rientranti nell'ambito della salvaguardia della sicurezza nazionale, ma certamente non tipici dell'attività propria degli organismi di *intelligence*. In questo senso, il presente decreto aggiorna nel rinnovato contesto istituzionale l'architettura di sicurezza cibernetica che era stata, da ultimo, definita con la Direttiva del Presidente del Consiglio dei ministri recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, adottata con decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017.

L'impianto normativo è improntato ai seguenti principali criteri:

- definizione delle competenze in materia di cybersicurezza del Vertice politico;
- razionalizzazione delle competenze in materia di cybersicurezza, con particolare riferimento agli ambiti della sicurezza delle reti e dei sistemi informativi (NIS), del perimetro di sicurezza nazionale cibernetica, e della sicurezza delle comunicazioni elettroniche (TELCO), della sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture digitali delle pubbliche amministrazioni anche in relazione ai servizi cloud, delle certificazioni di cybersicurezza, nonché in materia di sistema pubblico per la gestione dell'identità digitale e di qualificazione dei prestatori di servizi fiduciari qualificati e dei gestori di posta elettronica certificata, attualmente attribuite ad una pluralità di soggetti istituzionali. Ciò, anche al fine di assicurare l'unicità istituzionale di indirizzo e di azione, spesso invocata dagli operatori coinvolti, nei confronti dei soggetti pubblici e privati interessati, con particolare riferimento alla definizione di misure di sicurezza, così come alle funzioni ispettive, accertative e sanzionatorie, in un ambito connotato da un elevato livello di complessità tecnica e giuridica;
- supporto dello sviluppo di capacità industriali, tecnologiche e scientifiche nel campo della cybersicurezza, in un'ottica di autonomia strategica nazionale ed europea nel settore, con un forte impulso a progetti finalizzati di ricerca applicata, al partenariato pubblico-privato, allo sviluppo di nuove realtà imprenditoriali, al rafforzamento delle piccole-medie imprese

attraverso l'indirizzo e il coordinamento di opportuni processi di trasferimento tecnologico tra ricerca e industria assicurando anche un coordinamento europeo con enti omologhi su questi temi;

- attuazione del Piano Nazionale di Ripresa e Resilienza, deliberato dal Consiglio dei ministri nella riunione del 29 aprile 2021, che prevede apposite progettualità nell'ambito della cybersicurezza – ivi compresa la costituzione di un'agenzia nazionale di cybersicurezza – quale fattore necessario per assicurare lo sviluppo e la crescita dell'economia e dell'industria nazionale, ponendo la cybersicurezza a fondamento della trasformazione digitale;
- stretto raccordo dell'Architettura di cybersicurezza nazionale con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge 3 agosto 2007, n. 124, a fronte di una chiara separazione di competenze a tutela della sicurezza nazionale nel dominio cibernetico e dell'attribuzione di poteri di controllo al Comitato parlamentare per la sicurezza della Repubblica (COPASIR), di cui all'articolo 30 della legge n. 124 del 2007;
- gestione coordinata, con i diversi attori coinvolti, delle attività di prevenzione, preparazione e risposta a situazioni di crisi, anche mediante la costituzione, nell'ambito dell'istituenda Agenzia, del Nucleo per la cybersicurezza.

L'**articolo 1** reca le principali definizioni dei termini e degli acronimi utilizzati nel presente decreto. In particolare, viene introdotta la definzione di "cybersicurezza", con cui si intende fare riferimento all'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone altresì la resilienza.

L'**articolo 2** introduce nuove competenze per il Presidente del Consiglio dei ministri, in materia di cybersicurezza e, in particolare:

- l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico;
- l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) di cui all'articolo 4;
- la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 5;
- il potere, sentito il Comitato interministeriale per la cybersicurezza (CIC) di cui all'articolo 4 del presente decreto, di adottare direttive per la cybersicurezza e di emanare ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale.

Al comma 3, poi, ai fini dell'esercizio delle funzioni di controllo del COPASIR, è previsto che il Presidente del Consiglio dei ministri informi preventivamente il presidente del Comitato parlamentare circa le nomine del direttore generale e del vice direttore generale dell'Agenzia.

L'**articolo 3** prevede la possibilità per il Presidente del Consiglio dei ministri di delegare le funzioni previste dal presente decreto, e non attribuitegli in via esclusiva, ad un Ministro senza portafoglio o ad un Sottosegretario di Stato. Al fine di assicurare un punto di riferimento e di responsabilità politica comune all'istituenda Architettura di cybersicurezza nazionale e al Sistema per l'informazione della sicurezza della Repubblica, già assicurata in parte dalle attribuzioni conferite al Presidente del Consiglio dei ministri, la disposizione individua tale figura nella medesima Autorità, ove istituita, di cui all'articolo 3 della legge 3 agosto 2007, n. 124 (l'Autorità delegata per la sicurezza della Repubblica). Viene quindi creato un punto di raccordo politico per le attività di sicurezza nazionale nello spazio cibernetico e, nello specifico, tra quelle nel campo della cybersicurezza e quelle nel campo delle attività di ricerca informativa proprie dell'*intelligence*.

L'**articolo 4** completa l'assetto di governance della nuova Architettura nazionale di cybersicurezza e della istituenda Agenzia per la cybersicurezza nazionale, prevedendo l'istituzione presso la Presidenza del Consiglio dei ministri del Comitato interministeriale per la cybersicurezza (CIC), con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. In particolare, vengono poi affidate al CIC tutte le funzioni di consulenza e proposta già attribuite al CISR dal decreto-legge perimetro e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge, in materia di determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica. 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, anche da regimi di elevata classifica di segretezza.

Al comma 3, è previsto che il Comitato sia presieduto dal Presidente del Consiglio dei ministri e che sia composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico, dal Ministro della transizione ecologica, dal Ministro delle infrastrutture e della mobilità sostenibili, dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale.
Viene poi previsto, al comma 5, che possano essere chiamati a partecipare alle riunioni del Comitato anche altri componenti del Consiglio dei ministri, il direttore generale del DIS, il direttore dell'AISE, il direttore dell'AISI, nonché altre autorità civili e militari di cui, di volta in volta, sia ritenuta necessaria la presenza in relazione alle questioni da trattare
Il supporto al Comitato sarà assicurato dell'Agenzia per la cybersicurezza nazionale, al cui Direttore generale vengono assegnate, al comma 4, le funzioni di segretario del Comitato stesso.

L'**articolo 5** reca le disposizioni istitutive dell'Agenzia per la cybersicurezza nazionale, specificandone le finalità principali, e cioè la tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.
All'Agenzia viene attribuita personalità giuridica di diritto pubblico e viene disposto che goda di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti di quanto previsto dal presente decreto.
La particolarità dell'ambito di attività nel quale sarà chiamata ad operare l'istituenda Agenzia – e cioè quello della tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico – e le interazioni che necessariamente avrà con il Sistema di informazione per la sicurezza della Repubblica, hanno portato a definire una disciplina speciale, con l'individuazione degli opportuni punti di equilibrio, attribuendo all'Agenzia una configurazione giuridica che non segue il modello delle agenzie di cui al decreto legislativo 30 luglio 1999, n. 300, quanto piuttosto quello definito dalla legge n. 124 del 2007 per il DIS, AISE e AISI, al quale sono stati apportati i necessari adattamenti conseguenti alla non appartenenza al Comparto *intelligence*.

Sono state poi considerate l'esigenza di assicurare un più diretto controllo e potere di indirizzo al Presidente del Consiglio dei ministri, l'esigenza di assicurare uno stretto raccordo con il Sistema di informazione per la sicurezza della Repubblica e, anche in relazione a ciò, il potere di controllo del COPASIR, nonché, infine, la circostanza che molte delle funzioni attribuite all'Agenzia, prime fra tutte quelle relative al CSIRT italiano, sono attualmente svolte dal DIS, nel cui ambito verrà altresì necessariamente individuata una quota di personale specializzato che transiterà nei nuovi ruoli dell'Agenzia.

Viene quindi previsto che l'Agenzia abbia sede in Roma e che il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, se ne avvalgano per l'esercizio delle competenze di cui al presente decreto.

Il comma 4 prevede che il direttore generale sia nominato tra soggetti appartenenti a una delle categorie di cui all'articolo 18, comma 2, della legge n. 400 del 1988, in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione e dispone che gli incarichi del direttore generale e del vice direttore generale abbiano una durata massima di quattro anni e che siano rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni. È infine previsto che il direttore generale dell'Agenzia sia il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, per quanto previsto dal presente decreto, che lo stesso direttore generale sia gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia e che ne abbia la rappresentanza legale.

Al comma 5, è quindi prevista la possibilità per l'Agenzia di richiedere, per lo svolgimento dei suoi compiti istituzionali, anche sulla base di base di apposite convenzioni e nel rispetto degli ambiti di precipua competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle Forze di polizia o di enti pubblici.

Infine, al comma 7, ai fini di assicurare l'esercizio delle funzioni di controllo del COPASIR, è stato previsto che il Comitato parlamentare possa chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza.

L'**articolo 6** reca disposizioni in materia di organizzazione dell'Agenzia, prevedendo l'adozione di un apposito regolamento che ne disciplini l'articolazione in Uffici di livello dirigenziale generale (fino ad un numero massimo di otto), nonché in articolazioni di livello dirigenziale non generale (fino ad un numero massimo di trenta). Viene quindi disposto che organi dell'istituenda Agenzia siano il direttore generale e il Collegio dei revisori dei conti e che il richiamato regolamento rechi, altresì, disposizioni in merito alle funzioni del direttore generale e del vice direttore generale dell'Agenzia, alla composizione e al funzionamento del Collegio dei revisori dei conti e all'istituzione di eventuali sedi secondarie.

Infine, il comma 3 detta le disposizioni per la procedura di adozione del regolamento di organizzazione, prevedendo che lo stesso sia adottato, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400. Anche il regolamento di cui all'articolo 6 viene adottato previo parere del COPASIR, sentito il CIC.

L'**articolo 7** declina, quindi, le funzioni attribuite all'istituenda Agenzia per la cybersicurezza nazionale.

Tra le principali funzioni individuate nell'ambito del comma 1, si evidenziano quelle di cui alla lettera *a)*, con cui all'Agenzia viene attribuita la qualifica di Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, il compito di assicurare il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e di promuovere la realizzazione di una cornice di sicurezza e resilienza cibernetiche in funzione dello sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Viene precisato che il richiamato coordinamento debba avvenire nel rispetto delle competenze attribuite dalla

normativa vigente ad altre amministrazioni (e ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge 1° aprile 1981, n. 121), nonché – in relazione alle reti, ai sistemi informativi e ai servizi informatici attinenti alla gestione delle informazioni classificate – che restano fermi quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, e le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge.

Alla lettera *d)*, viene poi previsto che l'Agenzia, per le finalità di cui al decreto legislativo NIS, oltre a subentrare nelle funzioni di CSIRT italiano e punto di contatto unico, già assicurate dal DIS, assuma, anche a tutela dell'unità giuridica dell'ordinamento, le funzioni di Autorità nazionale competente in materia di sicurezza delle reti e dei sistemi informativi. Tali funzioni sono, infatti, attualmente attribuite ad una pluralità di amministrazioni e, in relazione alle reti ed ai sistemi informativi nei settori dell'attività di assistenza sanitaria e della fornitura e distribuzione di acqua potabile, anche alle Regioni e alle Province autonome di Trento e di Bolzano (per un totale di oltre 20 differenti Autorità competenti NIS). L'istituenda Agenzia diviene, quindi, l'unico attore istituzionale competente in materia di sicurezza delle reti e dei sistemi informativi e, in particolare, della predisposizione delle linee guida per la notifica degli incidenti, dell'adozione degli orientamenti sulle circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti, dell'accertamento delle violazioni ed irrogazione delle sanzioni amministrative previste dallo stesso decreto legislativo NIS.
Allo stesso tempo, è stata comunque considerata l'importanza del contributo delle attuali autorità competenti NIS in termini di conoscenza degli operatori (il Ministero dello sviluppo economico, per il settore infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali; il Ministero delle infrastrutture e della mobilità sostenibili, per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada; 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; il Ministero della salute, per l'attività di assistenza sanitaria, 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 attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati delle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza; il Ministero della transizione ecologica per il settore energia, sottosettori energia elettrica, gas e petrolio; 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), è stato previsto nell'articolo 15, dedicato alle modificazioni da apportare al decreto legislativo NIS, che le stesse divengano "autorità di settore", con il compito di proporre all'autorità nazionale competente NIS-Agenzia nazionale per la cybersicurezza le variazioni all'elenco degli operatori dei servizi essenziali, secondo i criteri stabiliti dallo stesso decreto legislativo NIS. È quindi previsto che le autorità di settore collaborino con l'autorità nazionale competente NIS per l'adempimento degli obblighi della disciplina NIS e, 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.

Alla lettera *e)*, viene quindi attribuita all'Agenzia la qualità di Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e viene disposto che assuma tutti i compiti in materia di certificazione di sicurezza cibernetica già attribuiti al Ministero dello sviluppo economico dall'ordinamento vigente, compresi quelli relativi all'accertamento delle violazioni e

all'irrogazione delle sanzioni. È quindi previsto che nello svolgimento dei predetti compiti, l'Agenzia accrediti, ai sensi dell'articolo 60, comma 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di propria competenza, e deleghi, ai sensi dell'articolo 56, comma 6, lettera *b)*, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le proprie strutture accreditate di cui al punto 1), al rilascio del certificato europeo di sicurezza cibernetica.

Vengono poi recate, alle lettere *h)* ed *i)*, le opportune disposizioni volte ad attribuire all'Agenzia, nell'ambito del perimetro di sicurezza nazionale cibernetica, le funzioni in materia di certificazione di sicurezza cibernetica attribuite al Ministero dello sviluppo economico, trasferendo, pertanto, presso l'istituenda Agenzia il Centro nazionale di certificazione e valutazione (CVCN), nonché i compiti relativi all'accertamento delle violazioni e all'irrogazione delle sanzioni attribuiti allo stesso Dicastero, in relazione i soggetti privati, e alla Presidenza del Consiglio dei ministri, in relazione ai soggetti pubblici ed a quelli di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82 (codice dell'amministrazione digitale - CAD).

Alle lettera *m)*, è prevista l'attribuzione all'istituenda Agenzia delle funzioni attualmente svolte dall'Agenzia per l'Italia digitale in materia di sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture digitali delle pubbliche amministrazioni anche in relazione ai servizi *cloud* e all'adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del CAD.

Al fine di innalzare la resilienza del Paese, è quindi previsto alla lettera *o)* che l'Agenzia partecipi alle esercitazioni nazionali e internazionali che riguardino la simulazione di eventi di natura cibernetica

Alla lettera *p)*, è poi previsto che l'Agenzia promuova la definizione e il mantenimento di un quadro giuridico nazionale aggiornato e coerente nell'ambito della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tale riguardo, al fine di assicurare il più possibile la coerenza dell'ordinamento giuridico in materia, è previsto altresì che l'Agenzia esprima pareri, di carattere obbligatorio ma non vincolante, sulle iniziative legislative o regolamentari concernenti la cybersicurezza;
Sono quindi previste, alle lettere *r)*, *s)*, *t)*, *v)* e *z)*, specifiche disposizioni volte ad assicurare il coinvolgimento di soggetti pubblici e privati nazionali, anche sulla base di apposite convenzioni, per lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche – anche mediante la promozione, lo sviluppo e il finanziamento di specifici progetti ed iniziative volti a favorire il trasferimento tecnologico dei risultati della ricerca nel settore della cybersicurezza – per la partecipazione dell'Italia a programmi, progetti e iniziative di cybersicurezza a livello UE e internazionale, per la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, nonché, infine, per la costituzione e la partecipazione a partenariati pubblico-privato sul territorio nazionale e, previa autorizzazione del Presidente del Consiglio dei ministri, ad enti, anche di forma societaria, congiuntamente a soggetti pubblici e privati. Infine, alla lettera *aa)*, è disposta la designazione dell'Agenzia quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento. Nel medesimo contesto, sempre al fine di dare attuazione alle disposizioni del richiamato regolamento (UE) 2021/887, è stabilito, al comma 2, che nell'ambito dell'Agenzia vengano nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Consiglio di direzione del citato Centro europeo.

Ai commi 3 e 4, è disposto il trasferimento presso l'Agenzia, rispettivamente, del CSIRT italiano, attualmente istituito presso il Dipartimento delle informazioni per la sicurezza, che assume la

denominazione di CSIRT Italia, e del Centro di valutazione e certificazione nazionale, attualmente istituito presso il Ministero dello sviluppo economico.

Infine, al comma 5, è prevista la possibilità che l'Agenzia consulti l'Autorità garante per la protezione dei dati personali e collabori con essa anche in relazione agli incidenti che comportino la violazione di dati personali, nel rispetto delle competenze della stessa Autorità. È quindi previsto che l'Agenzia e il Garante possano stipulare appositi protocolli d'intenti che definiscano altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.

Gli **articoli 8, 9 e 10** recano disposizioni in materia di Nucleo per la cybersicurezza e gestione delle crisi che coinvolgano aspetti di cybersicurezza. In particolare, viene dettata per la prima volta – dalla sua istituzione con la direttiva del Presidente del Consiglio dei ministri del 24 gennaio 2013 – la disciplina a livello legislativo del Nucleo per la sicurezza cibernetica, attualmente istituito presso il Dipartimento delle informazioni per la sicurezza in forza della direttiva del Presidente del Consiglio dei ministri del 17 febbraio 2017. Più nello specifico, il Nucleo per la sicurezza cibernetica assume la denominazione di Nucleo per la cybersicurezza e ne viene disposta l'istituzione presso l'Agenzia; ne viene aggiornata la composizione all'attuale configurazione del Governo (è prevista la partecipazione di un rappresentante, rispettivamente, del Ministro per la transizione ecologica, in virtù della sua partecipazione al Comitato interministeriale per la sicurezza della Repubblica di cui all'articolo 5 della legge n. 124 del 2007, e del Ministro per l'innovazione tecnologica e la transizione digitale); vengono definiti gli opportuni raccordi ordinamentali con le vigenti disposizioni in materia di convocazione del CISR in stato di crisi di cui all'articolo 7-*bis*, comma 5, del decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015, e di esercizio dei poteri del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge n. 105 del 2019, convertito, con modificazioni, dalla legge n. 133 del 2019 (istitutivo del perimetro di sicurezza nazionale cibernetica).

Con specifico riferimento alle situazioni di crisi, è salvaguardato e riaffermato il ruolo del CISR, anche in relazione all'esercizio dei richiamati poteri presidenziali di cui all'articolo 5 del decreto-legge n. 105 del 2019, ed è previsto che, per la gestione delle crisi che coinvolgano aspetti di cybersicurezza, il Nucleo assicuri il supporto al predetto Comitato interministeriale e al Presidente del Consiglio dei ministri, nonché assicuri le attività istruttorie e le procedure di attivazione necessarie.

L'**articolo 11** reca disposizioni in materia di contabilità e finanziarie.

In particolare, al comma 1, viene attribuita al Presidente del Consiglio dei ministri la determinazione del fabbisogno annuo delle risorse finanziarie dell'Agenzia, sulla base del quale verrà quindi determinato con legge di bilancio lo stanziamento annuale da assegnare all'Agenzia. È quindi disposto che del fabbisogno annuo venga data preventiva comunicazione al COPASIR.

Al comma 2, vengono specificate le fonti di entrata dell'istituenda Agenzia (tra cui, oltre alle dotazioni finanziarie e ai contributi ordinari di cui all'articolo 18 del presente decreto, i proventi derivanti dallo sfruttamento della proprietà industriale, dei prodotti dell'ingegno e delle invenzioni dell'Agenzia, i contributi dell'Unione europea o di organismi internazionali, ovvero i proventi delle sanzioni).

Al comma 3, vengono quindi recate le disposizioni in materia di regolamento di contabilità dell'Agenzia, prevedendo i criteri che il provvedimento di attuazione dovrà rispettare. Tra questi, assicurare l'autonomia gestionale e contabile dell'Agenzia, prevedere che i bilanci, preventivo e consuntivo, siano adottati dal direttore generale dell'Agenzia ed approvati, previo parere del CIC, con decreto del Presidente del Consiglio dei ministri, e che vengano sottoposti al controllo della Corte dei conti previsto dall'articolo 3, comma 4, della legge 14 gennaio 1994, n. 20. È quindi

disposto che il bilancio consuntivo venga trasmesso, insieme con la relazione della Corte dei conti, al COPASIR.

Infine, viene previsto al comma 4 che l'Agenzia, anche in deroga alle norme in materia di contratti pubblici, si doti di un regolamento che definisca le procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico e per quelle svolte in raccordo con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge n. 124 del 2007, ferma restando la disciplina di cui all'articolo 162 del decreto legislativo 18 aprile 2016, n. 50 (c.d. codice degli appalti pubblici).

L'**articolo 12** reca disposizioni in materia di personale, prevedendo che, con apposito regolamento venga dettata, nel rispetto dei principi generali dell'ordinamento giuridico, anche in deroga alle vigenti disposizioni di legge, ivi incluso il decreto legislativo 30 marzo 2001, n. 165, e nel rispetto dei criteri dettati dal presente decreto, la disciplina del contingente di personale addetto all'Agenzia.
A tale riguardo, il presente decreto prevede che il regolamento definisca l'ordinamento e il reclutamento del personale, il trattamento economico e previdenziale, prevedendo per il personale dell'Agenzia un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia, sulla scorta della equiparabilità delle funzioni svolte e del livello di responsabilità rivestito. La scelta di tale parametro retributivo è dovuta a diversi fattori, tra i quali: l'alta specializzazione richiesta dal personale che dovrà operare per l'istituenda Agenzia; le forti richieste da parte del mercato del lavoro, caratterizzate peraltro da offerte retributive particolarmente elevate – in particolare, da parte del settore privato, anche all'estero – cui è soggetto, nello specifico settore della cybersicurezza, il personale specializzato; l'esigenza di poter contare su un nucleo di personale strutturato e tendenzialmente con una permanenza nell'Agenzia di medio-lungo periodo, pur a fronte, come detto, di allettanti offerte professionali; l'alta specializzazione e la delicatezza delle funzioni di certificazione e vigilanza in settori particolarmente critici per il Paese (si considerino le certificazioni in ambito perimetro di sicurezza nazionale cibernetica e le attività di scrutinio tecnologico in materia di prodotti per la rete 5G nell'ambito dell'esercizio dei poteri speciali, c.d. *goden power*); da ultimo, la sensibilità del settore di attività nel quale verrà ad operare il personale dell'istituenda Agenzia, e cioè quello della sicurezza nazionale (nell'ambito cibernetico), anche in stretto raccordo con il Comparto *intelligence*, e delle attività riguardanti gli assetti tecnologici di soggetti pubblici e privati di primaria importanza per il Paese.
È quindi disposto, al comma 2, che il regolamento preveda, tra l'altro:

- la possibilità di procedere ad assunzioni a tempo determinato per specifiche progettualità e di avvalersi di un contingente di esperti, non superiore a cinquanta unità, in possesso di elevata competenza in materia di cyber sicurezza e di tecnologie digitali innovative, nello sviluppo e gestione di processi complessi di trasformazione tecnologica, nonché di significativa esperienza in progetti di trasformazione digitale. Tali disposizioni appaiono necessarie in ragione delle caratteristiche dell'attività che è chiamato a svolgere il personale dell'istituenda Agenzia, connotata da un elevato livello di preparazione tecnico-scientifica, e della necessità di poter affiancare al personale strutturato nei ruoli dell'Agenzia stessa, una quota di personale caratterizzata da un livello più elevato di *turn-over*;
- la possibilità di impiegare personale del Ministero della difesa, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri. Ciò anche in ragione dell'elevata professionalità ed esperienza del personale militare e dell'opportunità di un'osmosi sul piano tecnico tra l'istituenda Agenzia di cybersicurezza nazionale e la Difesa;
- le ipotesi di incompatibilità e le modalità applicative delle disposizioni del decreto legislativo 10 febbraio 2005, n. 30 (codice della proprietà industriale), ai prodotti dell'ingegno e alle invenzioni dei dipendenti dell'Agenzia.

Sono poi dettate disposizioni in materia di dotazione organica. Nello specifico, al comma 4 è previsto che, in sede di prima applicazione, il numero dei posti previsti dalla pianta organica sia di 300 unità, di cui fino a un massimo di 8 di livello dirigenziale generale, fino a un massimo di 24 di livello dirigenziale non generale e fino a un massimo di 268 di personale non dirigenziale.

Al comma 5 è, poi, previsto che, successivamente, la dotazione organica possa essere rideterminata, con decreti del Presidente del Consiglio dei ministri di concerto con il Ministro dell'economia e delle finanze, nei limiti delle risorse finanziarie destinate alle spese per il personale di cui all'articolo 18, comma 1. Ai fini dell'esercizio dei poteri di controllo del COPASIR, è quindi previsto che dei provvedimenti adottati in materia di dotazione organica dell'Agenzia sia data tempestiva e motivata comunicazione al presidente del Comitato parlamentare.

La previsione della possibilità che la forza organica dell'Agenzia possa essere rideterminata è legata alla quantità e qualità delle funzioni ad essa attribuita ed anche in considerazione delle dotazioni di personale delle agenzie di sicurezza cibernetica di altri importanti Paesi partner, quali Regno Unito (che, nel 2016, ha istituito il National Cyber Security Center con oltre 600 persone), Francia (ove opera l'ANSSI, istituita nel 2009 con circa 800 persone), Germania (dove è stato istituito nel 1991, con circa 1200 persone, il "*Bundesamt für Sicherheit in der Informationstechnik*"-BSI, l'Ufficio federale per la sicurezza informatica), Romania (che sta normando la propria Autorità di cybersicurezza con una previsione di impiego di 1250 persone entro il 2030).

Al comma 7 è previsto che, fatto salvo quanto disposto dall'articolo 42 della legge n. 124 del 2007, in materia di classifiche di segretezza, il personale che presta a qualsiasi titolo la propria opera alle dipendenze o in favore dell'Agenzia sia tenuto 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. Tale disposizione è volta ad assicurare l'imprescindibile riservatezza che deve connotare il personale dipendente dell'Agenzia, anche al fine di poter assicurare la necessaria fiducia da parte dei soggetti pubblici e privati interessati.

Al comma 8 sono quindi definite le procedure di adozione del regolamento in parola, prevedendo, anche in questo caso, la preventiva sottoposizione al parere del COPASIR.

L'**articolo 13** reca disposizioni in materia di trattamento dei dati personali. In particolare, è previsto che i trattamenti per finalità di sicurezza nazionale, in applicazione del presente decreto, siano svolti ai sensi dell'articolo 58, commi 2 e 3, del decreto legislativo 30 giugno 2003, n. 196. Resta inteso che, per tutti gli altri trattamenti, troverà applicazione la disciplina generale.

L'**articolo 14** è dedicato alle disposizioni in materia di obblighi informativi al Parlamento e, nello specifico, prevede che il Presidente del Consiglio dei ministri, entro il 30 aprile di ogni anno, trasmetta al Parlamento una relazione sull'attività svolta dall'Agenzia nell'anno precedente, in materia di cybersicurezza nazionale e che, entro il 30 giugno di ogni anno, il trasmetta al COPASIR, anche al fine di poter assicurare l'esercizio del potere di controllo sull'attività degli organismi di *intelligence* prevista dalla legge n. 124 del 2007, una relazione sulle attività svolte nell'anno precedente in raccordo con il Sistema di informazione per la sicurezza della Repubblica, nonché in relazione agli ambiti di attività dell'Agenzia sottoposti al controllo del medesimo Comitato ai sensi del presente decreto. La citata relazione annuale al Parlamento sostituisce l'attuale documento di sicurezza nazionale – concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali, nonché alla protezione cibernetica e alla sicurezza informatica – previsto dal comma 1-*bis* dell'articolo 38 della legge n. 124 del 2007, ed allegato alla relazione del Governo al Parlamento sulla politica dell'informazione per la sicurezza e sui risultati ottenuti, di cui allo stesso articolo 38.

L'**articolo 15** reca le modificazioni al decreto legislativo NIS funzionali a realizzare l'assetto istituzionale sopra descritto nella parte relativa all'articolo 7, comma 1, lettera *d)*. In particolare,

come detto, l'Agenzia assolverà le funzioni di autorità nazionale unica competente NIS, punto di contatto unico e di CSIRT. Conseguentemente, come già illustrato, saranno costitute le autorità di settore, con specifiche funzioni di proposta in merito all'aggiornamento dell'elenco degli operatori dei servizi essenziali, secondo i criteri stabiliti dallo stesso decreto legislativo NIS. Un'ulteriore modificazione riguarda la procedura di adozione della strategia nazionale di sicurezza cibernetica, ora strategia nazionale di cybersicurezza, per la quale è previsto che venga predisposta dall'Agenzia al fine di essere adottata dal Presidente del Consiglio dei ministri, sentito il CIC.

L'**articolo 16** contiene ulteriori, mirate, modificazioni normative conseguenti alle disposizioni introdotte dal presente decreto. In particolare, si fa riferimento alla legge n. 124 del 2007, al decreto-legge n. 105 del 2019, e relativi provvedimenti di attuazione, al decreto legislativo n. 104 del 2010, alla legge n. 53 del 2021, al decreto legislativo n. 179 del 2012 e, infine, al decreto legislativo n. 259 del 2003.

Le modifiche introdotte ai commi da 8 a 10 hanno lo scopo di assicurare che le disposizioni dirette a disciplinare il Centro di Valutazione e Certificazione Nazionale (CVCN) siano efficaci al momento della piena operatività del CVCN nonché di coordinare le procedure di cui all'articolo 1-bis "*Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G*" del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, con le disposizioni di cui all'articolo 3 decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

In particolare, la lettera a) del comma 6 dell'articolo 1 del d.l. n. 105 del 2019 è integrata prevedendo che l'obbligo della comunicazione dei soggetti inclusi nel Perimetro al CVCN è efficace a decorrere dal trentesimo giorno successivo alla pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana 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. Tale integrazione è finalizzata ad assicurare che il CVCN sia dotato delle risorse umane necessarie per l'avvio dell'operatività e per il corretto funzionamento delle procedure di valutazione previste.

Per quanto riguarda, invece, l'articolo 3 del d.l. n. 105 del 2019, si riporta di seguito la descrizione delle modifiche introdotte.

In primo luogo, si prevede l'abrogazione del comma 2, ai sensi del quale 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 di cui all'articolo 1, comma 6, lettera a), sulla base della disciplina prevista in attuazione del predetto regolamento. L'abrogazione in oggetto è strettamente collegata alla modifica introdotta con il comma 8, lett. a).

Inoltre, a decorrere dalla data in cui diviene efficace l'obbligo di comunicazione disciplinato dalla lettera a), sono apportate due ulteriori modifiche. Viene in primo luogo riformulato il primo comma dell'articolo 3, per chiarire innanzitutto che le disposizioni di cui all'articolo 1, comma 6, lettera a), del d.l. n. 105 del 2019, si applicano ai soggetti tenuti agli obblighi di cui all'articolo 1-bis del d.l. n. 21 del 2012, siano essi soggetti inclusi nel perimetro di sicurezza nazionale cibernetica o esclusi da esso. In particolare, si precisa che i soggetti che intendono procedere all'acquisizione, a qualsiasi titolo, di beni, servizi e componenti di cui all'articolo 1-*bis*, comma 2, del d.l. n. 21 del 2012, sono obbligati a effettuare la comunicazione di cui all'articolo 1, comma 6, lettera a), per lo svolgimento delle verifiche di sicurezza da parte del CVCN, condotte sulla base delle procedure, modalità e termini previsti dal regolamento di attuazione e che i fornitori di predetti beni, servizi e componenti sono tenuti a collaborare con il CVCN ai sensi dell'articolo 1, comma 6, lettera b). Viene quindi abrogato il comma 3 che prevede il riesame da parte del CVCN dei provvedimenti adottati ai sensi dell'articolo 1-*bis* della normativa Golden Power.

L'estensione dei tempi per l'applicazione dell'articolo non assicurerebbe infatti la necessaria certezza giuridica del quadro normativo, tenuto conto del fatto che si andrebbero a riesaminare prodotti e servizi già in uso da lungo tempo. D'altra parte, il CVCN seguirà un approccio graduale nell'esecuzione dei test per prodotti e servizi e pertanto eventuali verifiche potranno essere condotte in fase di vigilanza.

Il comma 10, introduce una modifica al comma 3-bis, dell'articolo 1-bis del d.l. n. 21 del 2012, con decorrenza dalla data in cui diviene efficace l'obbligo di comunicazione disciplinato dal comma 9, lettera a). Tali modifiche sono finalizzate al coordinamento delle procedure di valutazione del CVCN e quelle dell'esercizio dei poteri speciali di cui al comma 3-bis del predetto articolo 1-bis. Il comma prevede che entro dieci giorni dalla conclusione di un contratto l'impresa che ha acquisito, a qualsiasi titolo, i beni o i servizi notifichi alla Presidenza del Consiglio dei ministri un'informativa completa contenente anche la comunicazione del CVCN relativa all'esito della valutazione e alle eventuali prescrizioni e che entro trenta giorni dalla notifica, il Presidente del Consiglio dei ministri comunichi l'eventuale veto ovvero l'imposizione di specifiche prescrizioni o condizioni. In coerenza con tale proposta, il comma 1-bis specifica che, qualora il contratto sia stato stipulato antecedentemente alla conclusione dei test imposti dal CVCN (eventualità ammessa dall'articolo 1, comma 6, d.l. n. 105 del 2019), il termine di 10 giorni per effettuare la notifica golden power decorra non dalla data della stipulazione del contratto ma dalla comunicazione di esito positivo della valutazione effettuata dal CVCN.

Il comma 1-bis prevede inoltre l'eliminazione delle proroghe per "accertamenti tecnici", considerato che la valutazione del CVCN in merito ai profili di vulnerabilità tecnica sarà preventiva e assorbente rispetto a quella svolta da parte del Gruppo di coordinamento.

Da ultimo, analogamente a quanto previsto dall'articolo 1, comma 4 e dall'articolo 2, comma 4 del d.l. n. 21 del 2012, si specifica che il potere del Governo di ingiungere all'impresa il ripristino dello status quo ante può essere esercitato non soltanto nel caso di omessa notifica ma anche nel caso di violazione del contenuto prescrittivo del DPCM di esercizio dei poteri speciali. Conseguentemente il comma prevede di mantenere la formulazione "può ingiungere all'impresa di ripristinare a proprie spese la situazione anteriore", senza tuttavia la successiva specificazione "all'esecuzione del predetto contratto o accordo", atteso che l'inadempimento è necessariamente successivo all'esercizio dei poteri speciali e, quindi, all'inizio dell'esecuzione del contratto.

L'**articolo 17** introduce la possibilità per l'Agenzia di ricorrere all'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, per lo svolgimento delle funzioni ispettive ad essa attribuite, nonché per quelle relative all'attuazione e al controllo dell'esecuzione dei provvedimenti eventualmente assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro.

L'articolo prevede, altresì, che il personale dell'Agenzia, nello svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro, nonché delle funzioni relative al CSIRT Italia, rivesta la qualifica di pubblico ufficiale.

È quindi previsto che la trasmissione all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto-legge n. 144 del 2005, delle notifiche ricevute dal CSIRT Italia, costituisca, per il personale dell'Agenzia, al quale nello svolgimento delle funzioni relative al CSIRT Italia è riconosciuta la qualifica di pubblico ufficiale, adempimento dell'obbligo di denuncia da parte di pubblici ufficiali di cui all'art. 331 del codice di procedura penale.

Al fine di consentire l'attuazione delle disposizioni stabilite dal decreto, e un ordinato passaggio di funzioni, è poi stabilito, al comma 5, che con uno o più decreti di natura non regolamentare

del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, siano definiti i termini e le modalità:

- per assicurare la prima operatività dell'Agenzia, mediante l'individuazione di appositi spazi, in via transitoria e per un massimo di ventiquattro mesi, secondo opportune intese con le amministrazioni interessate;
- per il trasferimento, mediante opportune intese con le amministrazioni interessate, delle funzioni di cui all'articolo 7, nonché per il trasferimento dei beni strumentali e della documentazione, anche di natura classificata (si richiama, a titolo esemplificativo, che le funzioni di CSIRT italiano e quelle in materia di perimetro di sicurezza nazionale cibernetica, sono attualmente svolte da DIS e, pertanto, il relativo carteggio è soggetto al regime vigente, in generale, per tutta la documentazione del Dipartimento stesso).

Le funzioni che, ai sensi del presente decreto, sono oggetto di attribuzione all'Agenzia, resteranno pertanto assicurate dalle amministrazioni competenti sino al loro effettivo trasferimento, che avverrà, come sopra anticipato, secondo i termini e le modalità definite dai provvedimenti di cui al comma 5.

Sempre al fine di assicurare la prima operatività dell'Agenzia, al comma 7, è previsto che, dalla data di nomina del direttore generale dell'Agenzia, e fino all'adozione dei regolamenti di cui all'articolo 11, commi 3 e 5, il direttore generale dell'Agenzia identifichi e assuma gli impegni di spesa, che verranno liquidati a cura del DIS, nell'ambito delle risorse che verranno appositamente destinate all'Agenzia. Al fine di assicurare il controllo sull'attività contabile e finanziaria dell'Agenzia durante il periodo di avvio delle attività e nelle more dell'adozione dei richiamati regolamenti, è quindi disposto che, entro 90 giorni dall'approvazione dei medesimi regolamenti, delle spese effettuate ai sensi del comma 7, il Presidente del Consiglio dei ministri ne dia informazione al COPASIR.

Sono, poi, previste due disposizioni relative al personale. La prima, al comma 8, stabilisce che, in sede di prima applicazione delle disposizioni di cui al presente decreto e per un periodo massimo di sei mesi, prorogabile una sola volta per un massimo di ulteriori sei mesi, dalla data della nomina del direttore generale dell'Agenzia, l'ente si avvalga di un nucleo di personale, non superiore al 30 per cento della dotazione organica complessiva iniziale, di unità appartenenti al Ministero dello sviluppo economico, all'Agenzia per l'Italia digitale, al DIS, 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. Il relativo onere resta a carico dell'amministrazione di appartenenza. Tale disposizione è stata prevista per consentire all'Agenzia di poter iniziare ad operare fin da subito con un'aliquota di personale già impiegato, in particolare, nelle funzioni trasferite all'Agenzia stessa. La seconda, al comma 9, invece, stabilisce che il regolamento del personale di cui all'articolo 12 preveda apposite modalità selettive, per l'inquadramento – nella misura massima del 50 per cento della dotazione organica complessiva – del predetto personale, e di quello assunto a tempo determinato, ove già appartenente alla pubblica amministrazione, nel contingente di personale addetto all'Agenzia di cui al medesimo articolo 12, che tengano 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. A tale riguardo, è previsto che gli inquadramenti conseguenti alle richiamate procedure selettive, relative al personale di cui al comma 8, decorrano allo scadere dei sei mesi, ovvero della relativa proroga e, comunque, non oltre il 30 giugno 2022.

Le disposizioni in parola sono volte a non disperdere capacità specialistiche, non facilmente rinvenibili in un mercato del lavoro caratterizzato in questo settore da una grave carenza di specifiche professionalità, con conseguenti possibili riflessi sull'operatività dell'Agenzia.

È, infine, stabilito, al comma 10, che l'Agenzia si avvalga del patrocinio dell'Avvocatura dello Stato, ai sensi dell'articolo 1 del testo unico approvato con regio decreto 30 ottobre 1933, n. 1611.

L'**articolo 18** reca le disposizioni relative alla copertura finanziaria, illustrate in dettaglio in sede di relazione tecnica.

L'**articolo 19** disciplina l'entrata in vigore del decreto.

RELAZIONE TECNICA

(Articolo 17, comma 3, della legge 31 dicembre 2009 n. 196).

Articolo 1

Vengono introdotte le principali definizioni dei termini e degli acronimi utilizzati nel presente decreto.

Articoli da 2 a 4

Con le disposizioni di cui agli articoli da 2 a 4 viene definito il sistema di responsabilità e indirizzo sulle politiche nazionali di cybersicurezza. Nello specifico, vengono definite, nell'ambito definito dal presente decreto, le competenze del Presidente del Consiglio dei ministri, dell'Autorità delegata per la sicurezza della Repubblica di cui all'articolo 3 della legge n. 124 del 2007, ove istituita ai sensi della predetta legge, e del Comitato interministeriale per la cybersicurezza, istituito con il presente decreto. Si tratta di disposizioni ordinamentali, che non introducono nuovi o maggiori oneri per la finanza pubblica.

Articoli da 5 a 7

Con le disposizioni recate dagli articoli da 5 a 7 vengono disciplinate l'istituzione dell'Agenzia per la cybersicurezza nazionale, i criteri e le modalità per l'adozione del regolamento di organizzazione e le funzioni attribuite all'Agenzia stessa.

Con riferimento alle funzioni assegnate all'Agenzia, occorre evidenziare che molte di esse derivano dal trasferimento di funzioni già attribuite al Ministero per lo sviluppo economico, al Dipartimento delle informazioni per la sicurezza e all'Agenzia per l'Italia digitale.

I costi relativi al funzionamento dell'Agenzia sono riepilogati in tabella 1.

Per il 2021 è stato previsto uno stanziamento iniziale di 2 M€ per consentire le attività di avvio operativo dell'Agenzia nel corso dell'ultimo trimestre del 2021. Tale somma sarà utilizzata per coprire le spese relative agli emolumenti di un primo contingente di personale dell'Agenzia e di consulenti a contratto, oltre a coprire costi per trasferte, avvio dei servizi informatici, del supporto legale ed Amministrativo ed ogni altra attività funzionale alla partenza della nuova struttura.

Tabella 1: costi di funzionamento.

TOTALE COSTI GESTIONE OPERATIVA	2021	2022	2023	2024
Servizi informatici	€ 500.000,00	€ 14.000.000,00	€ 16.000.000,00	€ 16.000.000,00
Servizi professionali	€ 500.000,00	€ 4.000.000,00	€ 5.000.000,00	€ 5.000.000,00
Spese per il personale (tempo determinato e indet.)	€ 200.000,00	€ 20.000.000,00	€ 42.000.000,00	€ 58.000.000,00
Spese di funzionamento operativo	€ 800.000,00	€ 3.000.000,00	€ 7.000.000,00	€ 5.000.000,00
Totale	€ 2.000.000,00	€ 41.000.000,00	€ 70.000.000,00	€ 84.000.000,00

TOTALE COSTI GESTIONE OPERATIVA	2025	2026	2027
Servizi informatici	€ 16.000.000,00	€ 16.000.000,00	€ 16.000.000,00
Servizi professionali	€ 5.000.000,00	€ 5.000.000,00	€ 5.000.000,00
Spese per il personale (tempo determinato e indet.)	€ 74.000.000,00	€ 83.000.000,00	€ 95.000.000,00
Spese di funzionamento operativo	€ 5.000.000,00	€ 6.000.000,00	€ 6.000.000,00
Totale	€ 100.000.000,00	€ 110.000.000,00	€ 122.000.000,00

Articoli da 8 a 10

Le disposizioni, introducendo in via permanente presso l'Agenzia per la cybersicurezza nazionale il nuovo Nucleo per la cybersicurezza, compiono un ulteriore passo verso la ridefinizione dell'assetto dell'Architettura nazionale per la cybersicurezza, andando a inquadrare nel nuovo assetto istituzionale le funzioni già attribuite al Nucleo per la sicurezza cibernetica dalla Direttiva del Presidente del Consiglio dei ministri recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, adottata con decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017.

L'Agenzia, analogamente a quanto finora garantito dal DIS, assicurerà il supporto tecnico e organizzativo alle attività del Nucleo, nell'ambito delle risorse finanziarie umane e strumentali assegnate dal presente decreto, utilizzando personale che resterà comunque adibito anche allo svolgimento di altre funzioni ordinarie.

Per la partecipazione al Nucleo non sono previsti gettoni di presenza, compensi o rimborsi spese. La disposizione, pertanto, non introduce nuovi o maggiori oneri per la finanza pubblica.

Articolo 11

Al comma 1 viene previsto che con legge di bilancio è determinato lo stanziamento annuale da assegnare all'Agenzia da iscrivere sul capitolo di cui all'articolo 18, comma 1. Per la definizione del predetto stanziamento, compatibilmente con i saldi di finanza pubblica, occorre fare riferimento alle determinazioni del Presidente del Consiglio dei ministri, previamente comunicate al COPASIR.

Sono, poi, dettagliate le entrate dell'Agenzia, che saranno costituite da:

a) dotazioni finanziarie e contributi ordinari assegnati all'Agenzia;
b) corrispettivi per i servizi prestati a soggetti pubblici o privati;
c) proventi derivanti dallo sfruttamento della proprietà industriale, dei prodotti dell'ingegno e delle invenzioni dell'Agenzia;
d) altri proventi patrimoniali e di gestione;
e) contribuiti dell'Unione europea o di organismi internazionali, anche a seguito della partecipazione a specifici bandi, progetti e programmi di collaborazione;
f) proventi delle sanzioni 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;
g) ogni altra eventuale entrata.

La disposizione prevede, altresì, le modalità di adozione del regolamento di contabilità dell'Agenzia, nonché del regolamento che, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400 e alle norme in materia di contratti pubblici, previo parere del COPASIR e sentito il CICS, definisce le procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi, per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico e per quelle svolte in raccordo con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge n. 124 del 2007, ferma restando la disciplina di cui all'articolo 162 del decreto legislativo 18 aprile 2016, n. 50 (c.d. codice degli appalti pubblici).

Articolo 12

Le disposizioni stabiliscono che con apposito regolamento verrà dettata, anche in deroga alle vigenti disposizioni di legge e nel rispetto dei criteri di cui al presente decreto, la disciplina del contingente di personale addetto all'Agenzia. Sarà previsto per il personale dell'Agenzia un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia, sulla scorta della equiparabilità delle funzioni svolte e del livello di responsabilità rivestito. La norma precisa che la predetta equiparazione, sia con riferimento al trattamento economico in servizio che previdenziale, produce effetti avendo riguardo alle anzianità di servizio maturate a seguito dell'inquadramento nei ruoli dell'Agenzia.

Il regolamento determinerà, in particolare:

a) l'istituzione di un ruolo del personale e la disciplina generale del rapporto d'impiego alle dipendenze dell'Agenzia;
b) la possibilità di procedere, oltre che ad assunzioni a tempo indeterminato attraverso modalità concorsuali, ad assunzioni a tempo determinato, con contratti di diritto privato;

c) la possibilità di avvalersi, nei limiti delle disponibilità finanziarie dell'Agenzia, di un contingente di esperti. Il regolamento, disciplinerà le modalità di formazione del contingente e il compenso spettante per ciascuna professionalità;

In sede di prima applicazione delle disposizioni di cui al presente decreto, il numero di posti previsti dalla dotazione organica dell'Agenzia è individuato nella misura complessiva di trecento unità. Il regolamento individua quali delle disposizioni ivi contenute possono essere oggetto di revisione per effetto della negoziazione con le rappresentanze del personale.

È, infine, previsto un incremento della dotazione organica, con successivi decreti del Presidente del Consiglio dei ministri, adottati sentito il CICS, in relazione alle attività e competenze trasferite all'Agenzia, nei limiti delle risorse finanziarie ad essa destinate.

Articolo 13

Vengono dettate disposizioni in materia di trattamento dei dati personali da parte dell'Agenzia, con particolare riferimento ai trattamenti svolti per finalità di sicurezza nazionale in applicazione del presente decreto.

Articolo 14

Vengono dettate disposizioni in materia di controllo da parte del Parlamento sull'attività svolta dall'Agenzia in materia di cybersicurezza nazionale. Nello specifico, è prevista la presentazione di due relazioni, una al Parlamento e l'altra al COPASIR, sull'attività svolta dall'Agenzia nell'anno precedente, rispettivamente, in materia di cybersicurezza nazionale e sulle attività svolte in raccordo con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge n. 124 del 2007. Per l'assolvimento di tale obbligo informativo, l'Agenzia provvederà nell'ambito delle risorse finanziarie, umane e strumentali assegnate dal presente decreto.

Articolo 15

Le disposizioni recano le opportune modificazioni al decreto legislativo n. 65 del 2018 (recepimento della c.d. "direttiva NIS") conseguenti al passaggio all'Agenzia per la cybersicurezza nazionale delle funzioni attualmente attribuite ad altri enti e amministrazioni. Gli oneri derivanti dall'attuazione delle funzioni di cui agli articoli 7 e 8 del decreto legislativo n. 65 del 2018, che vengono attribuite all'Agenzia per la cybersicurezza nazionale, troveranno copertura secondo quanto disposto dall'articolo 22 del medesimo decreto legislativo.

Articolo 16

Vengono recate altre modificazioni conseguenti al nuovo assetto dell'Architettura nazionale di cybersicurezza. In particolare, vengono introdotte le modificazioni conseguenti al passaggio all'Agenzia per la cybersicurezza nazionale di tutte le competenze del DIS e del MiSE relative al decreto-legge "Perimetro" (D.L. n. 105/2019) e, in particolare, di quelle relative al CVCN, nonché di quelle di AgID.

Articolo 17

Vengono recate disposizioni transitorie e finali. In particolare, viene prevista la possibilità di fare ricorso da parte dell'Agenzia per la cybersicurezza nazionale all'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 per lo svolgimento delle funzioni ispettive attribuite all'Agenzia stessa, nonché per quelle relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro.

È, poi, stabilito che con uno o più decreti del Presidente del Consiglio dei ministri, di natura non regolamentare, sono definiti i termini e le modalità:

a) per assicurare la prima operatività dell'Agenzia, mediante l'individuazione di appositi spazi, in via transitoria e per un massimo di ventiquattro mesi, secondo opportune intese con le amministrazioni interessate, per l'attuazione delle disposizioni stabilite dal decreto;
b) per il trasferimento, mediante opportune intese con le amministrazioni interessate, delle funzioni di cui all'articolo 7, nonché per il trasferimento dei beni strumentali e della documentazione, anche di natura classificata, per l'attuazione delle disposizioni del presente decreto e la corrispondente riduzione di risorse finanziarie ed umane da parte delle amministrazioni cedenti.

Sempre al fine di assicurare la prima operatività dell'Agenzia, al comma 7, è previsto che, dalla data di nomina del direttore generale dell'Agenzia, e fino all'adozione dei regolamenti di cui all'articolo 11, commi 3 e 5, il direttore generale dell'Agenzia identifichi e assuma gli impegni di spesa, che verranno liquidati a cura del DIS, nell'ambito delle risorse che verranno appositamente destinate all'Agenzia. Al fine di assicurare il controllo sull'attività contabile e finanziaria dell'Agenzia durante il periodo di avvio delle attività e nelle more dell'adozione dei richiamati regolamenti, è quindi disposto che, entro 90 giorni dall'approvazione dei medesimi regolamenti, delle spese effettuate ai sensi del comma 7, il Presidente del Consiglio dei ministri ne dia informazione al COPASIR.

Vengono poi previste disposizioni in materia di personale, con particolare riferimento alla fase di prima applicazione del presente decreto e di avvio dell'attività dell'Agenzia per la cybersicurezza nazionale, i cui oneri trovano copertura secondo quanto illustrato in tabella 1.

Infine, viene previsto che l'Agenzia si avvale del patrocinio dell'Avvocatura dello Stato, ai sensi dell'articolo 1 del testo unico approvato con regio decreto 30 ottobre 1933, n. 1611.

Trattandosi di disposizioni di carattere ordinamentale e organizzatorio, non introducono nuovi o maggiori oneri per la finanza pubblica, rispetto a quelli già descritti in relazione all'articolo 12.

Articolo 18

La disposizione, al comma 1, prevede che per l'attuazione degli articoli da 5 a 7 è istituito, nello stato di previsione del Ministero dell'economia e delle finanze, un apposito capitolo con una dotazione di 2.000.000 di euro per l'anno 2021, 41.000.000 di euro per l'anno 2022, 70.000.000 di euro per l'anno 2023, 84.000.000 di euro per l'anno 2024, 100.000.000 di euro per l'anno 2025, 110.000.000 di euro per l'anno 2026 e 122.000.000 di euro annui a decorrere dall'anno 2027.

Ai predetti oneri si provvede mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190.

Al comma 3 è previsto che le risorse iscritte a legislazione vigente sui bilanci delle amministrazioni interessate, correlate alle funzioni ridefinite ai sensi del presente decreto a decorrere dall'entrata in servizio dell'Agenzia di cui all'articolo 5, sono accertate, anche in conto residui, con decreto del Ministro dell'economia e delle finanze, di concerto con i Ministri responsabili, e portate ad incremento del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190, anche mediante versamento all'entrata del bilancio dello Stato e successiva riassegnazione in spesa.

Il comma 4 prevede le modalità di riassegnazione a favore dell'Agenzia dei proventi di cui all'articolo 11, comma 2.

Infine, il comma 5, infine, prevede che il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, anche in conto residui, le occorrenti variazioni di bilancio per l'attuazione del presente decreto.

Articolo 19

La disposizione disciplina l'entrata in vigore del presente decreto.

La verifica della presente relazione tecnica, effettuata ai sensi e per gli effetti dell'art. 17, comma 3, della legge 31 dicembre 2009, n. 196 ha avuto esito

[X] POSITIVO [ ] NEGATIVO

Il Ragioniere Generale dello Stato

11 GIU. 2021

Decreto legge recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale

Articolo	Comma	Descrizione Norma	Spesa Entrata	Natura	Saldo netto da finanziare				Fabbisogno				Indebitamento netto			
					2021	2022	2023	2024	2021	2022	2023	2024	2021	2022	2023	2024
5-7	1	Agenzia per la cybersicurezza nazionale - Spese di funzionamento	s	c	1,8	21,0	28,0	26,0	1,8	21,0	28,0	26,0	1,8	21,0	28,0	26,0
5-7	1	Agenzia per la cybersicurezza nazionale - Spese di personale	s	c	0,2	20,0	42,0	58,0	0,2	20,0	42,0	58,0	0,2	20,0	42,0	58,0
5-7	1	Agenzia per la cybersicurezza nazionale - Effetti riflessi spese di personale	e	t/c					0,1	9,7	20,4	28,1	0,1	9,7	20,4	28,1
18	2	Riduzione Fondo esigenze indifferibili (art. 1, c. 200, legge 190/2014)	s	c	-2,0	-41,0	-70,0	-84,0	-2,0	-41,0	-70,0	-84,0	-2,0	-41,0	-70,0	-84,0
		TOTALE ENTRATE	**e**		**0,0**	**0,0**	**0,0**	**0,0**	**0,1**	**9,7**	**20,4**	**28,1**	**0,1**	**9,7**	**20,4**	**28,1**
		TOTALE SPESE	**s**		**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**	**0,0**
		TOTALE GENERALE ARTICOLATO			**0,0**	**0,0**	**0,0**	**0,0**	**0,1**	**9,7**	**20,4**	**28,1**	**0,1**	**9,7**	**20,4**	**28,1**

DICHIARAZIONE DI ESCLUSIONE DALL'AIR

MODULARIO P.C.M. 198

MOD. 251

Presidenza del Consiglio dei Ministri

DIPARTIMENTO PER GLI AFFARI GIURIDICI E LEGISLATIVI

Visto l'articolo 6, comma 1, lettera *c)*, del decreto del Presidente del Consiglio dei ministri 15 settembre 2017, n. 169, che dispone l'esclusione dall'AIR per i provvedimenti normativi concernenti "disposizioni direttamente incidenti su interessi fondamentali in materia di sicurezza interna ed esterna dello Stato";

Considerato che lo schema di decreto-legge recante disposizioni urgenti in materia di **cybersicurezza**, definizione dell'architettura nazionale di **cybersicurezza** ed istituzione dell'Agenzia per la **cybersicurezza** nazionale, concerne disposizioni necessarie per la sicurezza interna dello Stato;

SI DICHIARA

l'esclusione dall'AIR per lo schema di decreto-legge recante "Disposizioni urgenti in materia di **cybersicurezza**, definizione dell'architettura nazionale di **cybersicurezza** ed istituzione dell'Agenzia per la **cybersicurezza** nazionale".

Roma, 10.6.2021

Per delega del Capo del Dipartimento
Il dirigente generale
Dott. Edoardo Cervone

DISEGNO DI LEGGE

—

Art. 1.

1. È convertito in legge il decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

2. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale*.

Decreto-legge 14 giugno 2021, n. 82, pubblicato nella Gazzetta Ufficiale *n. 140 del 14 giugno 2021.*

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

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 77 e 87, quinto comma, della Costituzione;

Vista la legge 23 agosto 1988, n. 400, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri;

Considerato che le vulnerabilità delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche di soggetti pubblici e privati possono essere sfruttate al fine di provocare il malfunzionamento o l'interruzione, totali o parziali, di funzioni essenziali dello Stato e di servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, nonché di servizi di pubblica utilità, con potenziali gravi ripercussioni sui cittadini, sulle imprese e sulle pubbliche amministrazioni, sino a poter determinare un pregiudizio per la sicurezza nazionale;

Considerata la straordinaria necessità e urgenza, nell'attuale quadro normativo e a fronte della realizzazione in corso di importanti e strategiche infrastrutture tecnologiche, anche in relazione a recenti attacchi alle reti di Paesi europei e di importanti *partner* internazionali idonei a determinare effetti anche di natura sistemica e che sottolineano ulteriormente come il dominio cibernetico costituisca terreno di confronto con riflessi sulla sicurezza nazionale, di razionalizzare le competenze in materia, di assicurare un più efficace coordinamento, di attuare misure tese a rendere il Paese più sicuro e resiliente anche nel dominio digitale, di disporre dei più idonei strumenti di immediato intervento che consentano di affrontare con la massima efficacia e tempestività eventuali situazioni di emergenza che coinvolgano profili di cybersicurezza;

Considerata altresì la necessità e urgenza di dare attuazione al Piano nazionale di ripresa e resilienza, deliberato dal Consiglio dei ministri nella riunione del 29 aprile 2021, che prevede apposite progettualità nell'ambito della cybersicurezza, in particolare per l'istituzione di un'Agenzia di cybersicurezza nazionale, quale fattore necessario per tutelare la sicurezza dello sviluppo e della crescita dell'economia e dell'industria nazionale, ponendo la cybersicurezza a fondamento della trasformazione digitale;

Ritenuto pertanto di dover intervenire con urgenza al fine di ridefinire l'architettura italiana di cybersicurezza, prevedendo anche 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 di dover raccordare, altresì, pure a tutela dell'unità giuridica dell'ordinamento, le disposizioni in materia di sicurezza delle reti, dei sistemi informativi, dei servizi informatici e delle comunicazioni elettroniche;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 10 giugno 2021;

Sulla proposta del Presidente del Consiglio dei ministri;

EMANA

il seguente decreto-legge:

Articolo 1.

(Definizioni)

1. Ai fini del presente decreto si intende per:

a) cybersicurezza, l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità, e garantendone altresì la resilienza;

b) 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;

c) 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;

d) CISR, il Comitato interministeriale per la sicurezza della Repubblica di cui all'articolo 5 della legge 3 agosto 2007, n. 124;

e) DIS, il Dipartimento delle informazioni per la sicurezza di cui all'articolo 4 della legge n. 124 del 2007;

f) AISE, l'Agenzia informazioni e sicurezza esterna di cui all'articolo 6 della legge n. 124 del 2007;

g) AISI, l'Agenzia informazioni e sicurezza interna di cui all'articolo 7 della legge n. 124 del 2007;

h) COPASIR, il Comitato parlamentare per la sicurezza della Repubblica di cui all'articolo 30 della legge n. 124 del 2007;

i) strategia nazionale di cybersicurezza, la strategia di cui all'articolo 6 del decreto legislativo NIS.

Articolo 2.

(Competenze del Presidente del Consiglio dei ministri)

1. Al Presidente del Consiglio dei ministri sono attribuite in via esclusiva:

a) l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico;

b) l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) di cui all'articolo 4;

c) la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 5.

2. Ai fini dell'esercizio delle competenze di cui al comma 1, lett. *a)*, e dell'attuazione della strategia nazionale di cybersicurezza, il Presidente del Consiglio dei ministri, sentito il CIC, impartisce le direttive per la cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale.

3. Il Presidente del Consiglio dei ministri informa preventivamente il presidente del COPASIR circa le nomine di cui al comma 1, lettera c).

Articolo 3.

(Autorità delegata)

1. Il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare alla medesima Autorità di cui all'articolo 3 della legge n. 124 del 2007, ove istituita, le funzioni di cui al presente decreto che non sono ad esso attribuite in via esclusiva.

2. Il Presidente del Consiglio dei ministri è costantemente informato dall'Autorità delegata sulle modalità di esercizio delle funzioni delegate ai sensi del presente decreto e, fermo restando il potere di direttiva, può in qualsiasi momento avocare l'esercizio di tutte o di alcune di esse.

3. L'Autorità delegata, in relazione alle funzioni delegate ai sensi del presente decreto, partecipa alle riunioni del Comitato interministeriale per la transizione digitale di cui all'articolo 8 del decreto-legge 1° marzo 2021, n. 22, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 55.

Articolo 4.

(Comitato interministeriale per la cybersicurezza)

1. Presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la cybersicurezza (CIC), con funzioni di

consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

2. Il Comitato:

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

b) esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza;

c) promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza;

d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale.

3. Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico, dal Ministro della transizione ecologica, dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale e dal Ministro delle infrastrutture e della mobilità sostenibili.

4. Il direttore generale dell'Agenzia svolge le funzioni di segretario del Comitato.

5. Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, il direttore generale del DIS, il direttore dell'AISE, il direttore dell'AISI, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare.

6. Il Comitato svolge altresì le funzioni già attribuite al CISR dal decreto-legge perimetro e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge perimetro.

Articolo 5.

(Agenzia per la cybersicurezza nazionale)

1. È istituita, a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, l'Agenzia per la cybersicurezza nazionale, denominata ai fini del presente decreto « Agenzia », con sede in Roma.

2. 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 presente decreto. Il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono dell'Agenzia per l'esercizio delle competenze di cui al presente decreto.

3. Il direttore generale dell'Agenzia è nominato tra soggetti appartenenti a una delle categorie di cui all'articolo 18, comma 2, della legge n. 400 del 1988, in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione. Gli incarichi del direttore generale e del vice direttore generale hanno la durata massima di quattro anni e sono rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni. Il Direttore generale ed il vicedirettore generale, ove provenienti da pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, sono collocati fuori ruolo o in posizione di comando o altra analoga posizione, secondo gli ordinamenti di appartenenza. Per quanto previsto dal presente decreto, il direttore generale dell'Agenzia è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, ed è gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia. Il direttore generale ha la rappresentanza legale dell'Agenzia.

4. L'attività dell'Agenzia è regolata dal presente decreto e dalle disposizioni la cui adozione è prevista dallo stesso.

5. L'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di precipua competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle forze di polizia o di enti pubblici per lo svolgimento dei suoi compiti istituzionali.

6. Il COPASIR può chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza.

Articolo 6.

(Organizzazione dell'Agenzia per la cybersicurezza nazionale)

1. L'organizzazione e il funzionamento dell'Agenzia sono definiti da un apposito regolamento che ne prevede, in particolare, l'articolazione fino ad un numero massimo di otto uffici di livello dirigenziale generale, nonché fino ad un numero massimo di trenta articolazioni di livello dirigenziale non generale nell'ambito delle risorse disponibili.

2. Sono organi dell'Agenzia il direttore generale e il Collegio dei revisori dei conti. Con il regolamento di cui al comma 1 sono disciplinati altresì:

a) le funzioni del direttore generale e del vice direttore generale dell'Agenzia;

b) la composizione e il funzionamento del Collegio dei revisori dei conti;

c) l'istituzione di eventuali sedi secondarie.

3. Il regolamento di cui al comma 1 è adottato, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, previo parere del COPASIR, sentito il CIC.

Articolo 7.

(Funzioni dell'Agenzia per la cybersicurezza nazionale)

1. L'Agenzia:

a) è Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge 1° aprile 1981, n. 121, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, sia le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge n. 124 del 2007;

b) predispone la strategia nazionale di cybersicurezza;

c) svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza, di cui all'articolo 8;

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 NIS, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto;

e) è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:

1) accredita, ai sensi dell'articolo 60, comma 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali

organismi di valutazione della conformità per i sistemi di rispettiva competenza;

2) delega, ai sensi dell'articolo 56, comma 6, lettera *b)*, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate di cui al punto 1), 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, ivi comprese quelle relative:

1) al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto-legge perimetro, le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

2) alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui agli articoli 16-*bis* e 16-*ter* del decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

3) alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;

g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;

h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 131 del 2020;

i) assume tutte le funzioni già attribuite al DIS dal decreto-legge perimetro e dai relativi provvedimenti attuativi e supporta il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-*bis*, del decreto-legge perimetro;

l) provvede, sulla base delle attività di competenza del Nucleo per la cybersicurezza di cui all'articolo 8, alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro;

m) assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo. L'Agenzia assume, altresì, i compiti di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, già attribuiti all'Agenzia per l'Italia digitale;

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia di cui all'articolo 8 del decreto legislativo NIS;

o) partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

p) cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza;

q) coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della cybersicurezza. Nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni, ed enti, nonché segue nelle competenti sedi istituzionali le tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri;

r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza;

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 cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza, ferme restando le competenze del Ministero degli esteri e della cooperazione internazionale;

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza e dei correlati servizi applicativi, ferme restando le competenze del Ministero degli esteri e della cooperazione internazionale. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza;

u) svolge attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, 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 cybersicurezza, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati;

z) per le finalità di cui al presente articolo, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri.

aa) è designata quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

2. Nell'ambito dell'Agenzia sono nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Consiglio di direzione del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ai sensi dell'articolo 12 del regolamento (UE) 2021/887.

3. Il CSIRT italiano di cui all'articolo 8 del decreto legislativo NIS è trasferito presso l'Agenzia e assume la denominazione di: « CSIRT Italia ».

4. Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia.

5. Nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.

Articolo 8.

(Nucleo per la cybersicurezza)

1. Presso l'Agenzia è costituito, in via permanente, il Nucleo per la cybersicurezza, a supporto del Presidente del Consiglio dei ministri

nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

2. Il Nucleo per la cybersicurezza è presieduto dal direttore generale dell'Agenzia o dal vice direttore generale da lui designato ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, dell'AISE, dell'AISI, di ciascuno dei Ministeri rappresentati nel Comitato di cui all'articolo 5 della legge n. 124 del 2007, del Ministero dell'università e della ricerca, del Ministro delegato per l'innovazione tecnologica e la transizione digitale e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri. Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124 del 2007.

3. 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 cybersicurezza.

4. Il Nucleo può essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi di cui all'articolo 10.

Articolo 9.

(Compiti del Nucleo per la cybersicurezza)

1. Per le finalità di cui all'articolo 8, il Nucleo per la cybersicurezza svolge i seguenti compiti:

a) può formulare proposte di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia;

b) promuove, sulla base delle direttive di cui all'articolo 2, comma 2, la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile, anche nel quadro di quanto previsto dall'articolo 7-*bis*, comma 5, del decreto-legge n. 174 del 2015, convertito, con modificazioni, dalla legge n. 198 del 2015;

c) promuove e coordina lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

d) valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della cybersicurezza, procedure di condi-

visione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi;

e) riceve, per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi, dal DIS, dall'AISE e dall'AISI, dalle Forze di polizia e, in particolare, dall'organo del Ministero dell'interno di cui all'articolo 7-*bis* del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005, dalle strutture del Ministero della difesa, nonché dalle altre amministrazioni che compongono il Nucleo e dai gruppi di intervento per le emergenze informatiche (*Computer Emergency Response Team* – CERT) istituiti ai sensi della normativa vigente;

f) riceve dal CSIRT Italia le notifiche di incidente ai sensi delle disposizioni vigenti;

g) valuta se gli eventi di cui alle lettere *e)* e *f)* assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale, provvedendo in tal caso a informare tempestivamente il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla situazione in atto e allo svolgimento delle attività di raccordo e coordinamento di cui all'articolo 10, nella composizione ivi prevista.

Articolo 10.

(Gestione delle crisi che coinvolgono aspetti di cybersicurezza)

1. Nelle situazioni di crisi che coinvolgono aspetti di cybersicurezza, nei casi in cui il Presidente del Consiglio dei ministri convochi il CISR in materia di gestione delle predette situazioni di crisi, alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'Agenzia.

2. Il Nucleo assicura il supporto al CISR e al Presidente del Consiglio dei ministri, nella materia della cybersicurezza, per gli aspetti relativi alla gestione di situazioni di crisi ai sensi del comma 1, nonché per l'esercizio dei poteri attribuiti al Presidente del Consiglio dei ministri, ivi comprese le attività istruttorie e le procedure di attivazione necessarie, ai sensi dell'articolo 5 del decreto-legge perimetro.

3. In situazioni di crisi di natura cibernetica il Nucleo è integrato, in ragione della necessità, con un rappresentante, rispettivamente, del Ministero della salute, del Ministero delle infrastrutture e della mobilità sostenibili, 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, autorizzati ad assumere decisioni che impegnano la propria amministrazione. Alle riunioni i componenti possono farsi accompagnare da altri funzionari della propria amministrazione. Alle stesse 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.

4. È compito del Nucleo, nella composizione per la gestione delle crisi, di cui al comma 3, 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)*.

5. Il Nucleo, per l'espletamento delle proprie funzioni e fermo restando 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:

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.

Articolo 11.

(Norme di contabilità e disposizioni finanziarie)

1. Con legge di bilancio è determinato lo stanziamento annuale da assegnare all'Agenzia da iscrivere sul capitolo di cui all'articolo 18, comma 1, sulla base della determinazione del fabbisogno annuo operata dal Presidente del Consiglio dei ministri, previamente comunicata al COPASIR.

2. Le entrate dell'Agenzia sono costituite da:

a) dotazioni finanziarie e contributi ordinari di cui all'articolo 18 del presente decreto;

b) corrispettivi per i servizi prestati a soggetti pubblici o privati;

c) proventi derivanti dallo sfruttamento della proprietà industriale, dei prodotti dell'ingegno e delle invenzioni dell'Agenzia;

d) altri proventi patrimoniali e di gestione;

e) contribuiti dell'Unione europea o di organismi internazionali, anche a seguito della partecipazione a specifici bandi, progetti e programmi di collaborazione;

f) 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;

g) ogni altra eventuale entrata.

3. Il regolamento di contabilità dell'Agenzia, che ne assicura l'autonomia gestionale e contabile, 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 sentito il CIC, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e alle norme di contabilità generale dello Stato e nel rispetto dei princìpi fondamentali da esse stabiliti, nonché delle seguenti disposizioni:

a) il bilancio preventivo e il bilancio consuntivo adottati dal direttore generale dell'Agenzia sono approvati con decreto del Presidente del Consiglio dei ministri, previo parere del CIC e sono trasmessi alla Corte dei conti che esercita il controllo previsto dall'articolo 3, comma 4, della legge 14 gennaio 1994, n. 20;

b) il bilancio consuntivo e la relazione della Corte dei conti sono trasmessi, al COPASIR.

4. Con regolamento adottato con decreto del Presidente del Consiglio dei ministri, su proposta del direttore generale dell'Agenzia, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e alle norme in materia di contratti pubblici, previo parere del COPASIR e sentito il CIC, sono definite le procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico e per quelle svolte in raccordo con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge n. 124 del 2007, ferma restando la disciplina dell'articolo 162 del codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al decreto legislativo 18 aprile 2016, n. 50.

Articolo 12.

(Personale)

1. Con apposito regolamento è dettata, nel rispetto dei princìpi generali dell'ordinamento giuridico, anche in deroga alle vigenti disposizioni di legge, ivi incluso il decreto legislativo 30 marzo 2001, n. 165, e nel rispetto dei criteri di cui al presente decreto, la disciplina del contingente di personale addetto all'Agenzia, tenuto conto delle fun-

zioni di tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia e tenuto conto delle attività svolte dalla stessa in raccordo con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge n. 124 del 2007. Il regolamento definisce l'ordinamento e il reclutamento del personale, e il relativo trattamento economico e previdenziale, prevedendo, in particolare, per il personale dell'Agenzia un trattamento economico pari a quello in godimento da parte dei dipendenti della Banca d'Italia, sulla scorta della equiparabilità delle funzioni svolte e del livello di responsabilità rivestito. La predetta equiparazione, sia con riferimento al trattamento economico in servizio che previdenziale, produce effetti avendo riguardo alle anzianità di servizio maturate a seguito dell'inquadramento nei ruoli dell'Agenzia.

2. Il regolamento determina, nei limiti delle risorse finanziarie disponibili, in particolare:

a) l'istituzione di un ruolo del personale e la disciplina generale del rapporto d'impiego alle dipendenze dell'Agenzia;

b) 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, 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;

c) la possibilità di avvalersi di un contingente di esperti, non superiore a cinquanta unità, composto da personale collocato fuori ruolo o in posizione di comando o altra analoga posizione, prevista dagli ordinamenti di appartenenza, proveniente da pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche, ovvero da personale non appartenente alla pubblica amministrazione, in possesso di specifica ed elevata competenza in materia di cybersicurezza e di tecnologie digitali innovative, nello sviluppo e gestione di processi complessi di trasformazione tecnologica e delle correlate iniziative di comunicazione e disseminazione, nonché di significativa esperienza in progetti di trasformazione digitale, ivi compreso lo sviluppo di programmi e piattaforme digitali con diffusione su larga scala. Il regolamento, a tali fini, disciplina la composizione del contingente e il compenso spettante per ciascuna professionalità;

d) la determinazione della percentuale massima dei dipendenti che è possibile assumere a tempo determinato;

e) la possibilità di impiegare personale del Ministero della difesa, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri;

f) le ipotesi di incompatibilità;

g) le modalità di progressione di carriera all'interno dell'Agenzia;

h) 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;

i) le modalità applicative delle disposizioni del decreto legislativo 10 febbraio 2005, n. 30, recante il Codice della proprietà industriale, ai prodotti dell'ingegno ed alle invenzioni dei dipendenti dell'Agenzia;

l) i casi di cessazione dal servizio del personale assunto a tempo indeterminato ed i casi di anticipata risoluzione dei rapporti a tempo determinato;

m) quali delle disposizioni possono essere oggetto di revisione per effetto della negoziazione con le rappresentanze del personale.

3. Qualora le assunzioni di cui al comma 2, lettera *b)*, riguardino professori universitari di ruolo o ricercatori universitari confermati si applicano le disposizioni di cui all'articolo 12 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, anche per quanto riguarda il collocamento in aspettativa.

4. In sede di prima applicazione delle disposizioni di cui al presente decreto, il numero di posti previsti dalla dotazione organica dell'Agenzia è individuato nella misura complessiva di trecento unità, di cui fino a un massimo di otto di livello dirigenziale generale, fino a un massimo di 24 di livello dirigenziale non generale e fino a un massimo di 268 unità di personale non dirigenziale.

5. 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 di cui all'articolo 18, comma 1. Dei provvedimenti adottati in materia di dotazione organica dell'Agenzia è data tempestiva e motivata comunicazione al presidente del COPASIR.

6. Le assunzioni effettuate in violazione delle disposizioni del presente decreto o del regolamento di cui al presente articolo sono nulle, ferma restando la responsabilità personale, patrimoniale e disciplinare di chi le ha disposte.

7. Fatto salvo quanto previsto dall'articolo 42 della legge n. 124 del 2007, il personale che presta comunque la propria opera alle dipendenze o in favore dell'Agenzia è tenuto, anche dopo la cessazione di tale attività, al rispetto del segreto su ciò di cui sia venuto a conoscenza nell'esercizio o a causa delle proprie funzioni.

8. Il regolamento di cui al comma 1 è adottato, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, previo parere del COPASIR e sentito il CIC.

Articolo 13.

(Trattamento dei dati personali)

1. Il trattamento dei dati personali svolto per finalità di sicurezza nazionale in applicazione del presente decreto è effettuato ai sensi

dell'articolo 58, commi 2 e 3, del decreto legislativo 30 giugno 2003, n. 196.

Articolo 14.

(Relazioni annuali)

1. Entro il 30 aprile di ogni anno, il Presidente del Consiglio dei ministri trasmette al Parlamento una relazione sull'attività svolta dall'Agenzia nell'anno precedente, in materia di cybersicurezza nazionale.

2. Entro il 30 giugno di ogni anno, il Presidente del Consiglio dei ministri trasmette al COPASIR una relazione sulle attività svolte nell'anno precedente dall'Agenzia in raccordo con il Sistema di informazione per la sicurezza della Repubblica di cui alla legge n. 124 del 2007, nonché in relazione agli ambiti di attività dell'Agenzia sottoposti al controllo del Comitato ai sensi del presente decreto.

Articolo 15.

(Modificazioni al decreto legislativo NIS)

1. Al decreto legislativo NIS, sono apportate le seguenti modificazioni:

a) all'articolo 1, comma 2, lettera *a)*, le parole: « strategia nazionale di sicurezza cibernetica » sono sostituite dalle seguenti: « strategia nazionale di cybersicurezza »;

b) all'articolo 1, comma 2, lettera *b)*, le parole: « delle autorità nazionali competenti » sono sostituite dalle seguenti: « dell'autorità nazionale competente NIS, delle autorità di settore »;

c) all'articolo 3, lettera *a)*, le parole da: « autorità competente NIS » a: « per settore, » sono sostituite dalle seguenti: « autorità nazionale competente NIS, l'autorità nazionale unica, competente »;

d) all'articolo 3, dopo la lettera *a)*, è inserita la seguente: « *a*-bis*)* autorità di settore, le autorità di cui all'articolo 7, comma 1, lettere da *a)* a *e)* »;

e) all'articolo 4, il comma 6 è sostituito dal seguente:

« *6*. L'elenco degli operatori di servizi essenziali identificati ai sensi del 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 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. »;

f) all'articolo 6, nella rubrica, le parole: « sicurezza cibernetica » sono sostituite dalle seguenti: « cybersicurezza »; ai commi 1, 2 e 3, le parole: « sicurezza cibernetica » sono sostituite dalla seguente: « cybersicurezza »; al comma 4, le parole: « La Presidenza del Consiglio dei ministri » sono sostituite dalle seguenti: « L'Agenzia per la cybersicurezza » e le parole: « sicurezza cibernetica » sono sostituite dalle seguenti: « cybersicurezza »;

g) l'articolo 7 è sostituito dal seguente:

« Art. 7. – *(Autorità nazionale competente e punto di contatto unico)* – *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 infrastrutture digitali, sottosettori IXP, DNS, TLD, nonché per i servizi digitali;

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;

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 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;

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. 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. 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 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 effettivo, efficiente e sicuro con i rappresentanti designati dagli altri Stati.

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 collabora con essi.

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. »;

h) all'articolo 8, comma 1, le parole da: « la Presidenza » a: « la sicurezza » sono sostituite dalle seguenti: « l'Agenzia di cybersicurezza nazionale »;

i) l'articolo 9, comma 1, è sostituito dal seguente:

« *1*. Le autorità di settore collaborano con l'autorità nazionale competente NIS per l'adempimento degli obblighi 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. »;

l) all'articolo 12, comma 5, le parole da: « e, per conoscenza, » a: « NIS, » sono soppresse;

m) all'articolo 14, comma 4, le parole da: « e, per conoscenza, » a: « NIS, » sono soppresse;

n) all'articolo 19, comma 1, le parole: « dalle autorità competenti NIS » sono sostituite dalle seguenti: « dall'autorità nazionale competente NIS »;

o) all'articolo 19, il comma 2 è abrogato;

p) all'articolo 20, comma 1, le parole da: « Le autorità competenti NIS » a: « sono competenti » sono sostituite da: « L'autorità nazionale competente NIS è competente »;

q) all'allegato I:

1) al punto 1, dopo la lettera *d)* è aggiunta la seguente: « *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) al punto 2, lettera *c)*, dopo la parola: « standardizzate » sono inserite le seguenti: « , secondo le migliori pratiche internazionalmente riconosciute, ».

2. Nel decreto legislativo NIS:

a) ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, 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;

b) ogni riferimento al DIS, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale;

c) ogni riferimento alle autorità competenti NIS, ovunque ricorra, deve intendersi riferito all'autorità nazionale competente NIS, fatta eccezione per le disposizioni di cui all'articolo 5, comma 1, del medesimo decreto legislativo;

d) all'articolo 5, comma 1, alinea, le parole: « le autorità competenti NIS » sono sostituite dalle seguenti: « l'autorità nazionale competente NIS e le autorità di settore »;

e) agli articoli 6 e 12, le parole: « Comitato interministeriale per la sicurezza della Repubblica (CISR) » sono sostituite dalle seguenti: « Comitato interministeriale per la cybersicurezza (CIC) ».

Articolo 16.

(Altre modificazioni)

1. All'articolo 3, comma 1-*bis*, della legge n. 124 del 2007, dopo le parole: « della presente legge » sono aggiunte le seguenti: « e in materia di cybersicurezza ».

2. All'articolo 38 della legge n. 124 del 2007, il comma 1-*bis* è abrogato.

3. La denominazione: « CSIRT Italia » sostituisce, ad ogni effetto e ovunque presente in provvedimenti legislativi e regolamentari, la denominazione: « CSIRT Italiano ».

4. Nel decreto-legge perimetro 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 », fatta eccezione per le disposizioni di cui all'articolo 5 del medesimo decreto-legge.

5. Nel decreto-legge perimetro ogni riferimento al Dipartimento delle informazioni per la sicurezza, o al DIS, ovunque ricorra, è da intendersi riferito all'Agenzia per la cybersicurezza nazionale e ogni riferimento al Nucleo per la sicurezza cibernetica è da intendersi riferito al Nucleo per la cybersicurezza.

6. Nel decreto-legge perimetro:

a) ogni riferimento al Ministero dello sviluppo economico e alla Presidenza del Consiglio dei ministri, ovunque ricorra, è da intendersi riferito all'Agenzia per la cybersicurezza nazionale;

b) all'articolo 1, comma 8, lettera *a)*, le parole da: « definite dalla Presidenza del Consiglio dei ministri » a: « decreto legislativo 18 maggio 2018, n. 65 » sono sostituite dalle seguenti: « definite dall'Agenzia per la cybersicurezza nazionale »;

c) all'articolo 1, comma 8, lettera *b)*, le parole: « all'autorità competente » sono sostituite dalle seguenti: « autorità nazionale competente NIS ».

7. Nei provvedimenti di natura regolamentare e amministrativa la cui adozione è prevista dall'articolo 1 del decreto-legge perimetro, ogni riferimento al CISR e al DIS deve intendersi rispettivamente riferito al CIC e all'Agenzia per la cybersicurezza nazionale.

8. Nei provvedimenti di natura regolamentare e amministrativa la cui adozione è prevista dall'articolo 1 del decreto-legge perimetro, ogni riferimento al Ministero dello sviluppo economico e alla struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale, fatta eccezione per le disposizioni di cui agli articoli 3 del decreto del Presidente del Consiglio dei ministri n. 131 del 2020.

9. Al decreto-legge perimetro sono apportate le seguenti modificazioni:

a) all'articolo 1, comma 6, lettera *a)*, dopo il primo periodo è inserito il seguente: « L'obbligo di comunicazione di cui alla presente lettera è efficace a decorrere dal trentesimo giorno successivo alla pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana 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. »;

b) all'articolo 3, il comma 2 è abrogato;

c) a decorrere dalla data in cui diviene efficace l'obbligo di comunicazione disciplinato dalla lettera *a)*, all'articolo 3:

1) il comma 1 è sostituito dal seguente: « *1*. I soggetti che intendono procedere all'acquisizione, a qualsiasi titolo, di beni, servizi e componenti di cui all'articolo 1-*bis*, comma 2, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, sono obbligati ad effettuare la comunicazione di cui all'articolo 1, comma 6, lettera *a)*, per lo svolgimento delle verifiche di sicurezza da parte del CVCN sulla base delle procedure, modalità e

termini previsti dal regolamento di attuazione. Ai fornitori di predetti beni, servizi e componenti si applica l'articolo 1, comma 6, lettera *b)*. »;

2) il comma 3 è abrogato;

10. A decorrere dalla data in cui diviene efficace l'obbligo di comunicazione disciplinato dal comma 9, lettera *a)*, al decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, il comma 3-*bis* dell'articolo 1-*bis* è sostituito dal seguente: « *3-bis*. Entro dieci giorni dalla conclusione di un contratto o accordo di cui al comma 2, l'impresa che ha acquisito, a qualsiasi titolo, i beni o i servizi di cui allo stesso comma notifica alla Presidenza del Consiglio dei ministri un'informativa completa, contenente anche la comunicazione del Centro di valutazione e certificazione nazionale (CVCN), relativa all'esito della valutazione e alle eventuali prescrizioni, in modo da consentire l'eventuale esercizio del potere di veto o l'imposizione di specifiche prescrizioni o condizioni. Qualora il contratto sia stato stipulato antecedentemente alla conclusione dei test imposti dal CVCN, il termine di cui al primo periodo decorre dalla comunicazione di esito positivo della valutazione effettuata dal CVCN. Entro trenta giorni dalla notifica, il Presidente del Consiglio dei ministri comunica l'eventuale veto ovvero l'imposizione di specifiche prescrizioni o condizioni. I poteri speciali sono esercitati nella forma dell'imposizione di specifiche prescrizioni o condizioni ogniqualvolta ciò sia sufficiente ad assicurare la tutela degli interessi essenziali della difesa e della sicurezza nazionale. Decorsi i predetti termini, i poteri speciali si intendono non esercitati. Qualora si renda necessario richiedere informazioni all'acquirente, tale termine è sospeso, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di dieci giorni. Qualora si renda necessario formulare richieste istruttorie a soggetti terzi, il predetto termine di trenta giorni è sospeso, per una sola volta, fino al ricevimento delle informazioni richieste, che sono rese entro il termine di venti giorni. Le richieste di informazioni e le richieste istruttorie a soggetti terzi successive alla prima non sospendono i termini. In caso di incompletezza della notifica, il termine di trenta giorni previsto dal presente comma decorre dal ricevimento delle informazioni o degli elementi che la integrano. Fermo restando quanto previsto in materia di sanzioni al presente comma, nel caso in cui l'impresa notificante abbia iniziato l'esecuzione del contratto o dell'accordo oggetto della notifica prima che sia decorso il termine per l'esercizio dei poteri speciali, ovvero abbia eseguito il contratto o accordo in violazione del decreto di esercizio dei poteri speciali, il Governo può ingiungere all'impresa di ripristinare a proprie spese la situazione anteriore. Salvo che il fatto costituisca reato, chiunque non osservi gli obblighi di notifica di cui al presente articolo ovvero le disposizioni contenute nel provvedimento di esercizio dei poteri speciali è soggetto alla sanzione amministrativa pecuniaria fino al 150 per cento del valore dell'operazione e comunque non inferiore al 25 per cento del medesimo valore. Nei casi di violazione degli obblighi di notifica di cui al presente articolo, anche in assenza della notifica, la Presidenza del Consiglio dei ministri può avviare il procedimento ai fini dell'eventuale esercizio dei poteri speciali. A tale scopo, trovano applicazione i termini

e le norme procedurali previsti dal presente comma. Il termine di trenta giorni di cui al presente comma decorre dalla conclusione del procedimento di accertamento della violazione dell'obbligo di notifica ».

11. All'articolo 135 del decreto legislativo 2 luglio 2010, n. 104, dopo la lettera *h)*, è aggiunta la seguente: « *h-bis)* le controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale; ».

12. Alla legge 22 aprile 2021, n. 53, sono apportate le seguenti modificazioni:

a) all'articolo 4, comma 1, lettera *b)*, dopo le parole: « Ministero dello sviluppo economico » sono aggiunte le seguenti: « e l'Agenzia per la cybersicurezza nazionale »;

b) all'articolo 18, ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale.

13. All'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, le parole: « L'AgID » sono sostituite dalle seguenti: « L'Agenzia per la cybersicurezza nazionale ».

14. Al decreto legislativo 1° agosto 2003, n. 259, sono apportate le seguenti modificazioni:

a) agli articoli 16-*bis* e 16-*ter*, ogni riferimento al Ministero dello sviluppo economico, ovunque ricorra, deve intendersi riferito all'Agenzia per la cybersicurezza nazionale;

b) all'articolo 16-*ter*, comma 1, le parole: « Ministro dello sviluppo economico » sono sostituite dalle seguenti: « Presidente del Consiglio dei ministri »;

c) all'articolo 16-*ter*, comma 2, lettera *b)*, le parole: « , in collaborazione con gli Ispettorati territoriali del Ministero dello sviluppo economico, » sono soppresse.

Articolo 17.

(Disposizioni transitorie e finali)

1. Per lo svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, di cui all'articolo 7, l'Agenzia può provvedere, oltre che con proprio personale, con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

2. Per lo svolgimento delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro, l'Agenzia provvede con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio

2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

3. Il personale dell'Agenzia, nello svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, di cui all'articolo 7, nonché delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro, riveste la qualifica di pubblico ufficiale.

4. Il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale. La trasmissione delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, costituisce adempimento dell'obbligo di cui all'articolo 331 del codice di procedura penale.

5. Con uno o più decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, da adottare entro centottanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, sono definiti i termini e le modalità:

a) per assicurare la prima operatività dell'Agenzia, mediante l'individuazione di appositi spazi, in via transitoria e per un massimo di ventiquattro mesi, secondo opportune intese con le amministrazioni interessate, per l'attuazione delle disposizioni del presente decreto;

b) mediante opportune intese con le amministrazioni interessate, per il trasferimento delle funzioni di cui all'articolo 7, nonché per il trasferimento dei beni strumentali e della documentazione, anche di natura classificata, per l'attuazione delle disposizioni del presente decreto e la corrispondente riduzione di risorse finanziarie ed umane da parte delle amministrazioni cedenti.

6. In relazione al trasferimento delle funzioni di cui all'articolo 7, comma 1, lettera *m*), dall'AgID all'Agenzia, i decreti di cui al comma 5 definiscono, altresì, i raccordi tra le due amministrazioni, per le funzioni che restano di competenza di AgID.

7. Al fine di assicurare la prima operatività dell'Agenzia, il direttore generale dell'Agenzia, fino all'adozione dei regolamenti di cui all'articolo 11, commi 3 e 5, 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, commi 3 e 5, delle spese effettuate ai sensi del presente comma, il Presidente del Consiglio dei ministri ne dà informazione al COPASIR.

8. In sede di prima applicazione delle disposizioni di cui al presente decreto e per un periodo massimo di sei mesi, prorogabile una sola volta per un massimo di ulteriori sei mesi, dalla data della nomina del direttore generale dell'Agenzia, l'Agenzia si avvale di un nucleo di personale, non superiore al 30 per cento della dotazione organica complessiva iniziale, di unità appartenenti al Ministero dello sviluppo economico, all'Agenzia per l'Italia digitale, al DIS, 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. Il relativo onere resta a carico dell'amministrazione di appartenenza.

9. Il regolamento di cui all'articolo 12, comma 1, prevede apposite modalità selettive per l'inquadramento, nella misura massima del 50 per cento della dotazione organica complessiva, del personale di cui al comma 8 e del personale di cui all'articolo 12, comma 2, lettera *b)*, ove già appartenente alla pubblica amministrazione, nel contingente di personale addetto all'Agenzia di cui al medesimo articolo 12, che tengano 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. Gli inquadramenti conseguenti alle procedure selettive di cui al presente comma, relative al personale di cui al comma 8, decorrono allo scadere dei sei mesi o della relativa proroga e, comunque, non oltre il 30 giugno 2022.

10. L'Agenzia si avvale del patrocinio dell'Avvocatura dello Stato, ai sensi dell'articolo 1 del testo unico approvato con regio decreto 30 ottobre 1933, n. 1611.

Articolo 18.

(Disposizioni finanziarie)

1. Per l'attuazione degli articoli da 5 a 7 è istituito, nello stato di previsione del Ministero dell'economia e delle finanze, un apposito capitolo con una dotazione di 2.000.000 di euro per l'anno 2021, 41.000.000 di euro per l'anno 2022, 70.000.000 di euro per l'anno 2023, 84.000.000 di euro per l'anno 2024, 100.000.000 di euro per l'anno 2025, 110.000.000 di euro per l'anno 2026 e 122.000.000 di euro annui a decorrere dall'anno 2027.

2. Agli oneri di cui al comma 1, si provvede mediante corrispondete riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190.

3. Le risorse iscritte sui bilanci delle amministrazioni interessate, correlate alle funzioni ridefinite ai sensi del presente decreto a decorrere dall'entrata in servizio dell'Agenzia di cui all'articolo 5, sono accertate, anche in conto residui, con decreto del Ministro dell'economia e delle finanze, di concerto con i Ministri responsabili, e portate ad incremento del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190, anche mediante versamento all'entrata del bilancio dello Stato e successiva riassegnazione in spesa.

4. I proventi di cui all'articolo 11, comma 2, sono versati all'entrata del bilancio dello Stato, per essere riassegnati al capitolo di cui al comma 1.

5. Ai fini dell'immediata attuazione delle disposizioni del presente decreto il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, anche in conto residui, le occorrenti variazioni di bilancio per l'attuazione del presente decreto.

Articolo 19.

(Entrata in vigore)

1. Il presente decreto entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana e sarà presentato alle Camere per la conversione in legge.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 14 giugno 2021

MATTARELLA

DRAGHI, *Presidente del Consiglio dei ministri*

Visto, *il Guardasigilli:* CARTABIA