COMMISSIONI RIUNITE

I (Affari costituzionali, della Presidenza del Consiglio e interni) e IX (Trasporti, poste e telecomunicazioni)

S O M M A R I O

SEDE REFERENTE

Martedì 22 giugno 2021. — Presidenza della presidente della IX Commissione Raffaella PAITA. – Interviene il Ministro per i rapporti con il Parlamento Federico D'Incà.

La seduta comincia alle 14.35.

DL 82/2021: Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.
C. 3161 Governo.

(Esame e rinvio).

Le Commissioni iniziano l'esame del provvedimento.

Raffaella PAITA, *presidente*, avverte innanzitutto che, come specificato anche nelle convocazioni, alla luce di quanto stabilito dalla Giunta per il Regolamento nella riunione del 4 novembre scorso, i deputati possono partecipare all'odierna seduta in sede referente in videoconferenza, in quanto nella seduta odierna non sono previste votazioni sul provvedimento.

Rileva quindi come le Commissioni riunite I e IX avviino nella seduta odierna l'esame, in sede referente, del disegno di legge di 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.

Giuseppe BRESCIA (M5S), *relatore per la I Commissione*, rileva innanzitutto come, in considerazione dell'accresciuta esposizione alle minacce cibernetiche si sia imposta nell'agenda nazionale ed internazionale la necessità di sviluppare, in tempi brevi, idonei e sempre più stringenti meccanismi di tutela. Tale esigenza è emersa con forza negli ultimi anni anche alla luce delle misure normative volte a garantire infrastrutture *cloud* sicure e centri dati con elevati standard di qualità nella direzione di una crescente interoperabilità e condivisione delle informazioni.

A livello di Unione europea richiama la direttiva (UE) 2016/1148 del 6 luglio 2016, la quale reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (cosiddetta direttiva NIS – *Network and Information Secu-*

rity) al fine di conseguire un « livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea ».

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

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

Segnala quindi come la sicurezza cibernetica costituisca uno degli interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021.

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

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

Passando ad illustrare il contenuto delle singole disposizioni del decreto-legge, per quanto riguarda gli articoli da 1 a 4 e da 13 a 19, l'articolo 1 reca le definizioni utilizzate nel provvedimento.

L'articolo 2, comma 1, prevede, alla lettera *a)*, che il Presidente del Consiglio dei ministri è l'autorità al vertice dell'architettura della sicurezza cibernetica, in quanto a lui è attribuita in via esclusiva l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

Inoltre, al Presidente del Consiglio spetta, sempre in via esclusiva: ai sensi della lettera b), l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) istituito all'articolo 4 del provvedimento; ai sensi della lettera *c)*, la nomina e la revoca del direttore generale e del vice direttore generale della nuova Agenzia per la cybersicurezza nazionale istituita dall'articolo 5 del provvedimento in esame.

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

In tale contesto l'articolo 4, comma 6, provvede a trasferire al predetto CIC le funzioni già attribuite al CISR dal decreto-legge n. 105 del 2019 e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge n. 105 del 2019.

Ai sensi del comma 2, il Presidente del Consiglio, ai fini dell'esercizio delle com-

petenze di responsabilità generale e dell'attuazione della strategia nazionale di cybersicurezza, impartisce le direttive per la cybersicurezza ed emana le disposizioni per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale, previo parere del CIC.

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

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

Ai sensi del comma 2, in caso di nomina dell'Autorità delegata, questa è tenuta a informare costantemente sulle modalità di esercizio delle funzioni delegate il Presidente del Consiglio, il quale, « fermo restando il potere di direttiva », può in qualsiasi momento avocare a sé l'esercizio di tutte o di alcune di esse.

In base al comma 3, l'Autorità delegata, in relazione alle funzioni delegate, partecipa alle riunioni del Comitato interministeriale per la transizione digitale di cui all'articolo 8 del decreto-legge n. 22 del 2021. A tale riguardo ricorda che il Comitato interministeriale per la transizione digitale, istituito dal richiamato decreto-legge n. 22 del 2021, è la sede di coordinamento e monitoraggio dell'attuazione delle iniziative di innovazione tecnologica e transizione digitale delle pubbliche amministrazioni competenti in via ordinaria.

L'articolo 4, al comma 1, istituisce, presso la Presidenza del Consiglio dei ministri, il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

Il comma 2 attribuisce al CIC i seguenti compiti: proporre al Presidente del Consiglio gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale; esercitare l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza; promuovere l'adozione delle iniziative per favorire la collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza; esprimere il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale.

Ai sensi del comma 3 il Comitato è composto: dal Presidente del Consiglio (che lo presiede); 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; dal Ministro delle Infrastrutture e della mobilità sostenibili.

Ai sensi del comma 4, le funzioni di segretario del Comitato sono svolte dal direttore generale dell'Agenzia per la cybersicurezza nazionale.

Il comma 5 prevede che possono partecipano alle sedute del Comitato, su chiamata del Presidente del Consiglio, 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; altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare.

Come già anticipato, il comma 6 trasferisce al CIC le funzioni già attribuite al CISR dal decreto-legge n. 105 del 2019 (« decreto-legge perimetro ») e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge n. 105 del 2019.

Ricorda in merito che il suddetto articolo 5, nel cui ambito restano in capo al

CISR le attuali previsioni, prevede che, in caso di rischio grave ed imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, il Presidente del Consiglio, previa deliberazione del CISR, può disporre la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati.

Per quanto riguarda le altre funzioni in materia di perimetro di sicurezza cibernetica, inizialmente attribuite al CISR e ora trasferite al CIC in base al decreto-legge, richiama il compito di proporre al Presidente del Consiglio l'adozione degli atti attuativi (alcuni attuati, altri ancora da adottare) del decreto-legge n. 105 del 2019 e di proporre al Presidente del Consiglio l'individuazione dell'elenco (e il suo aggiornamento periodico) dei soggetti inclusi nel perimetro di sicurezza cibernetica (articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019).

Oltre alle misure previste dal « decreto-legge perimetro », sulle competenze poste originariamente in capo al CISR e ora trasferite al CIC interviene altresì l'articolo 15 del decreto-legge, modificando le previsioni del decreto legislativo n. 65 del 2018 che ha dato attuazione alla direttiva NIS.

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

L'articolo 14 prevede, al comma 1, la trasmissione entro il 30 aprile di ogni anno di una relazione al Parlamento sull'attività svolta dall'Agenzia nell'anno precedente in materia di cybersicurezza nazionale.

Il comma 2 prevede inoltre che il Presidente del Consiglio dei ministri trasmetta al Copasir, entro il 30 giugno di ogni anno, una relazione sulle attività svolte nell'anno precedente dall'Agenzia 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 Comitato medesimo ai sensi del decreto-legge in esame.

L'articolo 15 modifica il decreto legislativo n. 65 del 2018, che ha dato attuazione alla direttiva (UE) 2016/1148 (cosiddetta direttiva *Network and Information Security* – NIS), e che rappresenta la cornice legislativa delle misure per la sicurezza delle reti e dei sistemi informativi e dei soggetti competenti a dare attuazione agli obblighi previsti in tale ambito.

Rammenta che la citata direttiva ha previsto misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione al fine di conseguire un « livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea ».

Le modifiche recate dall'articolo 15 sono volte ad adeguare il decreto legislativo n. 65 del 2018 alle previsioni del decreto-legge, alla luce della nuova architettura delineata dal provvedimento.

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

In particolare, il comma 1 modifica l'articolo 3, comma 1-*bis*, della legge n. 124 del 2007 che, nel testo previgente, non consente all'Autorità delegata per la sicurezza della Repubblica di esercitare funzioni di governo ulteriori rispetto a quelle ad essa delegate dal Presidente del Consiglio dei ministri nell'ambito del sistema di informazioni per la sicurezza della Repubblica a norma della medesima legge 124. La disposizione consente all'Autorità delegata di svolgere anche le funzioni « in materia di cybersicurezza ». La modifica è posta in relazione con l'articolo 3 del decreto in esame che dà facoltà al Presidente del

Consiglio di delegare le competenze in materia di cybersicurezza alla medesima Autorità delegata per la sicurezza della Repubblica, se istituita.

Il comma 2 abroga il comma 1-*bis* dell'articolo 38 della legge n. 124 del 2007, il quale prevedeva che alla relazione sulla politica dell'informazione per la sicurezza e sui risultati ottenuti, sia allegato il documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica. La modifica è conseguente a quanto disposto dall'articolo 14, che dispone in ordine alla trasmissione di due relazioni annuali in materia di cybersicurezza.

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

I commi da 4 a 7 recano una serie di modifiche alla legislazione vigente dovute al trasferimento di competenze operate dal provvedimento in esame.

I commi 8 e 9 recano disposizioni di modifica del decreto-legge n. 105 del 2019 volte ad adeguare le disposizioni di tale decreto-legge alle modifiche intervenute.

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

Il comma 10 modifica, al fine di integrarle con il riferimento ai test effettuati dal CVCN, le disposizioni del decreto-legge n. 21 del 2012 in merito alle comunicazioni da effettuare a cura delle imprese acquirenti impianti per il 5G ai fini dell'esercizio dei poteri speciali, prevedendo inoltre alcune integrazioni e alcune semplificazioni procedurali.

Il comma 11 inserisce tra le competenze del Tribunale amministrativo regionale del Lazio, sede di Roma, anche le controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale.

I commi 12, 13 e 14 aggiornano al nuovo quadro normativo, con particolare riferimento alle funzioni della citata Agenzia per la cybersicurezza nazionale, le disposizioni della legge di delegazione europea 2019-2020, quelle relative alla definizione della competenza regolamentare in materia di sicurezza e qualità delle infrastrutture digitali per la pubblica amministrazione e del Codice delle Comunicazioni elettroniche.

L'articolo 17 reca una serie di disposizioni transitorie e finali, prevedendo, al comma 1, che per lo svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, attribuite alla neo-istituita Agenzia per la cybersicurezza nazionale, essa possa avvalersi « dell'ausilio » del personale dell'organo centrale del Ministero dell'interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni (previsto dall'articolo 7-*bis* del decreto-legge n. 144 del 2005; ossia il Servizio di polizia postale e delle comunicazioni del Dipartimento della pubblica sicurezza).

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

Il comma 3 stabilisce che il « personale dell'Agenzia », nello svolgimento delle funzioni richiamato nei commi 1 e 2 del medesimo articolo 17, riveste la qualifica di pubblico ufficiale.

Il comma 4 concerne il personale dell'Agenzia addetto al CSIRT Italia (trasferito presso l'Agenzia dall'articolo 7), stabilendo che anche questo personale, nello svolgimento delle proprie funzioni, riveste la qualifica di pubblico ufficiale.

Il comma 5 demanda ad uno o più decreti del Presidente del Consiglio dei ministri la definizione di termini e di modalità per assicurare la prima operatività dell'Agenzia, onde trasferire funzioni, beni stru-

mentali e documentazione, attuare le disposizioni del decreto-legge, regolare le riduzioni di risorse finanziarie relative alle amministrazioni cedenti. I decreti devono essere adottati entro centottanta giorni dall'entrata in vigore del decreto-legge. Circa la prima operatività dell'Agenzia, si prevedono intese con le amministrazioni interessate, nonché l'individuazione di appositi spazi in via transitoria.

Ai sensi del comma 6, con decreto del Presidente del Consiglio dei ministri è altresì definito il dovuto raccordo tra la neoistituita Agenzia e l'Agenzia per l'Italia digitale (AgID), per quanto concerne il trasferimento di funzioni da questa a quella previsto dall'articolo 7.

Il comma 7 prevede che il direttore generale dell'Agenzia identifichi e assuma impegni di spesa, che il Dipartimento delle informazioni per la sicurezza liquida nell'ambito delle risorse destinate appunto all'Agenzia. Questo, fino all'adozione di un regolamento di contabilità dell'Agenzia che ne assicuri l'autonomia gestionale e contabile, e di un regolamento sulle procedure per la stipula di contratti di appalti di lavori e forniture di beni (atti previsti dall'articolo 11 del decreto-legge).

Il comma 8 concerne l'inizio dell'operatività della nuova Agenzia sotto il profilo delle dotazioni di organico e dei relativi oneri, prevedendo che per un periodo massimo di sei mesi – prorogabile una sola volta, per un massimo di ulteriori sei mesi – l'Agenzia si avvalga di personale appartenente al Ministero dello sviluppo economico, all'Agenzia per l'Italia digitale, al Dipartimento delle informazioni per la sicurezza, 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. Numericamente, il personale esterno temporaneamente a disposizione dell'Agenzia non può eccedere il 30 per cento della dotazione organica complessiva iniziale dell'Agenzia stessa. I relativi oneri sono a carico delle amministrazioni di appartenenza.

Il comma 9 dispone che il regolamento disciplinante l'ordinamento e il reclutamento del personale addetto all'Agenzia (previsto dall'articolo 12 del decreto-legge) preveda modalità selettive per l'inquadramento – nella misura massima del 50 per cento della dotazione organica complessiva – del personale di primo avvalimento (ai sensi del comma 8) o del personale assunto a tempo determinato (ai sensi dell'articolo 12, comma 2, lettera *b)*, ove già appartenente a pubbliche amministrazioni. Le modalità selettive tengono conto delle mansioni svolte e degli incarichi ricoperti durante il periodo di servizio presso l'Agenzia, nonché delle competenze possedute e dei requisiti di professionalità ed esperienza richiesti per le specifiche posizioni. Ove si tratti del personale di primo avvalimento (ai sensi del comma 8), gli inquadramenti conseguenti alle procedure selettive decorrono allo scadere dei sei mesi, o della relativa proroga, e comunque, non oltre il 30 giugno 2022.

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

L'articolo 18 reca le disposizioni finanziarie per l'attuazione degli articoli da 5 a 7 del decreto-legge, prevedendo, al comma 1, l'istituzione di un capitolo dedicato all'Agenzia nello stato di previsione del Ministero dell'economia e delle finanze, la cui dotazione è pari a: 2 milioni per il 2021; 41 milioni per il 2022; 70 milioni per il 2023; 84 milioni per il 2024; 100 milioni per il 2025; 110 milioni per il 2026; 122 milioni a decorrere dall'anno 2027.

Ai sensi del comma 2 a tali oneri si provvede mediante corrispondente riduzione del Fondo per far fronte ad esigenze indifferibili che si manifestano nel corso della gestione, istituito (ai sensi dell'articolo 1, comma 200, della legge n. 190 del 2014) nello stato di previsione del Ministero dell'economia e delle finanze.

In base ai commi 3 e 4 a tale Fondo si prevede affluiscano, in via incrementale, le

risorse iscritte sui bilanci delle amministrazioni interessate, correlate alle funzioni attribuite all'Agenzia, le quali sono accertate, anche in conto residui, con decreto del Ministro dell'economia e delle finanze (di concerto con i Ministri responsabili), per essere riassegnate al capitolo istituito dal comma 1.

L'articolo 19 concerne l'entrata in vigore del decreto-legge, stabilita per il giorno successivo a quello della pubblicazione: il decreto-legge è dunque vigente dal 15 giugno 2021.

Raffaella PAITA, *presidente e relatrice per la IX Commissione*, avverte che nella sua relazione si soffermerà sulle norme che istituiscono l'Agenzia per la cybersicurezza nazionale, determinandone le funzioni e l'organizzazione.

L'articolo 5 istituisce per l'appunto l'Agenzia per la cybersicurezza nazionale, che ha sede a Roma, a tutela degli interessi nazionali nel campo della cybersicurezza, nonché della sicurezza nazionale nello spazio cibernetico.

L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. L'istituzione dell'Agenzia è strumentale all'esercizio delle competenze che il decreto-legge assegna al Presidente del Consiglio dei ministri e all'Autorità delegata, ove istituita.

Il comma 3 riguarda il direttore generale dell'Agenzia, che ne rappresenta l'organo di gestione, stabilendo in particolare che tale figura è il legale rappresentante dell'Agenzia ed è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata.

Il direttore dell'Agenzia è nominato dal Presidente del Consiglio dei Ministri ed è scelto dallo stesso tra le categorie tra cui può essere nominato il segretario generale della Presidenza del Consiglio ossia: magistrati delle giurisdizioni superiori ordinaria ed amministrativa, avvocati dello Stato, dirigenti generali dello Stato ed equiparati, professori universitari di ruolo ovvero tra estranei alla pubblica amministrazione. La disposizione richiede altresì il possesso di una documentata esperienza di elevato livello nella gestione dei processi di innovazione.

L'incarico del direttore ha una durata massima di 4 anni e può essere rinnovato, anche con successivi provvedimenti, per un massimo di ulteriori 4 anni. Anche per il vicedirettore generale è stabilita la medesima durata.

Per lo svolgimento dei suoi compiti istituzionali, l'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di rispettiva competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle forze di Polizia o di enti pubblici. È inoltre previsto che il Copasir « può chiedere l'audizione » del direttore generale dell'Agenzia su questioni di propria competenza.

L'articolo 6 prevede che l'Agenzia, la cui organizzazione e funzionamento sono definiti da un apposito regolamento, è articolata in uffici di livello dirigenziale generale, che il decreto-legge stabilisce nel numero massimo di otto, e in uffici di livello dirigenziale non generale, fino ad un massimo di trenta.

Gli organi dell'Agenzia sono costituiti dal direttore generale, che rappresenta l'organo di gestione, e dal collegio dei revisori dei conti, quale organo di controllo interno; si prevede inoltre che le funzioni del direttore generale e del vicedirettore generale siano disciplinate nel regolamento di organizzazione dell'Agenzia.

La lettera *b)* del comma 2 rinvia per la composizione ed il funzionamento del collegio interamente al predetto regolamento di organizzazione.

La lettera *c)* del comma 2 stabilisce che il regolamento di organizzazione può prevedere l'istituzione di sedi secondarie.

Il regolamento è adottato, entro centoventi giorni dalla data di entrata in vigore della legge di conversione del decreto-legge, 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 n. 400 del 1988, previo parere del COPASIR, sentito il CIC.

L'articolo 7 determina le funzioni della « Agenzia per la cybersicurezza nazionale »,

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

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

All'Agenzia, in base al comma 1, sono in particolare attribuite le funzioni che seguono.

Ai sensi della lettera *a)*, l'Agenzia è Autorità nazionale per la cybersicurezza, e pertanto le spetta il coordinamento tra i soggetti pubblici coinvolti nella cybersicurezza a livello nazionale; in tale ruolo essa promuove azioni comuni dirette ad assicurare la sicurezza cibernetica, a sviluppare la digitalizzazione del sistema produttivo e delle pubbliche amministrazioni e del Paese, nonché a conseguire autonomia (nazionale ed europea) per i prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore. Rimane salvo – per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate – quanto previsto dal regolamento adottato ai sensi della legge n. 124 del 2007 sul « Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto »; rimangono inoltre ferme le competenze dell'Ufficio centrale per la segretezza; rimane altresì fermo che il Ministero dell'interno sia l'autorità nazionale di pubblica sicurezza titolare delle correlative attribuzioni.

Ai sensi della lettera *b)*, l'Agenzia « predispone » la strategia nazionale di cybersicurezza.

Ai sensi della lettera *c)*, essa svolge ogni necessaria attività di supporto al funzionamento del « Nucleo per la cybersicurezza ».

Ai sensi della lettera *d)*, l'Agenzia è Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo n. 65 del 2018, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto legislativo.

Ai sensi della lettera e), è l'Autorità nazionale di certificazione della cybersicurezza.

Ai sensi della lettera *f)*, assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico. Ne segue che sono traslate all'Agenzia le competenze di quest'ultimo Ministero, relative, tra l'altro, al perimetro di sicurezza nazionale cibernetica, alla sicurezza ed integrità delle informazioni elettroniche, alla sicurezza delle reti e dei sistemi informativi. Per quanto concerne il perimetro di sicurezza nazionale cibernetica – oggetto del decreto-legge n. 105 del 2019 – tale trasferimento di funzioni investe altresì le attività di verifica e ispezione dei privati (attribuite al predetto Ministero dall'articolo 1, comma 6, lettera *c)*, del decreto-legge n. 105); inoltre esso concerne le funzioni attribuite al Centro di valutazione e certificazione nazionale (CVCN) presso il Ministero dello sviluppo economico (di cui all'articolo 1, comma 6, lettera *a)*, del decreto-legge n. 105, che all'articolo 2 aveva autorizzato a tal fine l'assunzione fino a 77 unità di personale a tempo indeterminato presso il Ministero), il quale viene trasferito dal comma 4 dell'articolo 7 del decreto-legge presso l'Agenzia.

Ai sensi della lettera *g)*, l'Agenzia partecipa (per gli ambiti di competenza) al gruppo di coordinamento istituito dalle disposizioni attuative del decreto-legge n. 21 del 2012, recante norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strate-

gica nei settori dell'energia, dei trasporti e delle comunicazioni.

Ai sensi della lettera *h)*, essa assume le funzioni in materia di perimetro di sicurezza nazionale cibernetica attribuite alla Presidenza del Consiglio, individuate dal decreto-legge n. 105 del 2019. Tra queste rientrano l'accertamento delle violazioni e l'irrogazione delle sanzioni amministrative per i soggetti pubblici (nonché i gestori di servizi fiduciari qualificati o di posta elettronica) che facciano parte del perimetro; sono tuttavia mantenute in capo alla Presidenza del Consiglio le funzioni attribuitegli dall'articolo 3 del citato DPCM n. 131 del 2021, circa l'individuazione dei soggetti rientranti nel perimetro, per il settore spazio e aerospazio e per il settore tecnologie critiche (e la struttura della Presidenza del Consiglio competente alla innovazione tecnologica e digitalizzazione vi è prevista agire « in raccordo » con il Ministero per lo sviluppo economico, per il settore servizi digitali).

Ai sensi della lettera *i)*, l'Agenzia assume tutte le funzioni già attribuite al Dipartimento delle informazioni per la sicurezza dal citato decreto-legge n. 105 del 2019. Pertanto è da ritenersi che la neo-istituita Agenzia sia chiamata a stabilire misure che garantiscano elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici rientranti nel perimetro, e divenga destinataria delle notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici; ai sensi della disposizione, inoltre, l'Agenzia, in luogo del Dipartimento, supporta il Presidente del Consiglio dei ministri, a fini di coordinamento dell'attuazione della disciplina del perimetro nazionale.

Ai sensi della lettera *l)*, l'Agenzia provvede alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge n. 105 del 2019, il quale prevede che il Presidente del Consiglio – in presenza di un rischio grave e imminente per la sicurezza nazionale, connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici – possa disporre la disattivazione di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati, secondo un criterio di proporzionalità, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione.

Ai sensi della lettera *m)*, l'Agenzia assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale.

Ai sensi della lettera *n)*, essa sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici. A tal fine l'Agenzia si avvale anche del CSIRT Italia (previsto dall'articolo 8 del decreto legislativo n. 65 del 2018 e la cui organizzazione è disciplinata dal DPCM 8 agosto 2019), il quale era istituito presso il Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio, ma che il comma 3 dell'articolo 7 del decreto-legge trasferisce presso l'Agenzia.

Ai sensi della lettera *o)*, l'Agenzia partecipa alle esercitazioni nazionali e internazionali in ordine alla simulazione di eventi di natura cibernetica, onde incrementare la « resilienza » del Paese.

Ai sensi della lettera *p)*, essa 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.

Ai sensi della lettera *q)*, l'Agenzia coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della cybersicurezza; per questo riguardo, l'Agenzia cura i rapporti con i competenti organismi dell'Unione europea ed internazionali.

Ai sensi della lettera *r)*, essa sostiene (negli ambiti di competenza) lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. In particolare, l'Agen-

zia si fa promotrice del coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionale e può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore.

Ai sensi della lettera *s)*, l'Agenzia 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.

Ai sensi della lettera *t)*, essa promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea ed internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali; rimangono ferme le competenze del Ministero degli esteri e della cooperazione internazionale.

Ai sensi della lettera *u)*, l'Agenzia svolge attività di comunicazione e promozione della « consapevolezza » in materia di cybersicurezza, « al fine di contribuire allo sviluppo di una cultura nazionale in materia ».

Ai sensi della lettera *v)*, essa 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.

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

Ai sensi della lettera *aa)*, l'Agenzia è designata come Centro nazionale di coordinamento, ai sensi del regolamento (UE) 2021/887, il quale istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

Il comma 2 dell'articolo 7 prevede, a tale ultimo riguardo, che il rappresentante dell'Italia (ed il suo supplente) entro il consiglio di direzione del Centro europeo siano nominati « nell'ambito dell'Agenzia », con decreto del Presidente del Consiglio.

Come già detto, il comma 3 prevede che il CSIRT italiano di cui all'articolo 8 del decreto legislativo « NIS » è trasferito presso l'Agenzia e assume la denominazione di: « CSIRT Italia », mentre il comma 4 stabilisce che è trasferito presso l'Agenzia il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico.

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

L'articolo 8 dispone la costituzione, presso l'Agenzia, di un Nucleo per la cybersicurezza, previsto in via permanente, quale supporto del Presidente del Consiglio riguardo alle tematiche della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

Ai sensi del comma 2, il Nucleo è presieduto dal direttore generale dell'Agenzia – o dal vice direttore generale da lui designato. Il Nucleo è composto: dal Consigliere militare del Presidente del Consiglio; da un rappresentante del Dipartimento dell'informazione per la sicurezza (DIS); da un rappresentante dell'Agenzia informazioni e sicurezza esterna (AISE); da un rappresentante dell'Agenzia informazioni e sicurezza interna (AISI); da un rappresentante di ciascuno dei Ministeri rappresentati nel Comitato interministeriale per la sicurezza (Affari esteri; Interno; Difesa; Giustizia; Economia e finanze; Sviluppo economico; Transizione ecologica); da un rappresentante di ciascuno dei seguenti Ministeri o Dipartimenti: Università e ricerca; Innovazione tecnologica e transizione digitale; Protezione civile; limitatamente alla

trattazione di informazioni classificate, da un rappresentante dell'Ufficio centrale per la segretezza.

Ai sensi del comma 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.

A fronte di questa composizione « allargata », il comma 4 prevede una possibile composizione « ristretta », con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi.

Segnala come la disposizione « legifichi » l'istituzione del Nucleo, attualmente previsto dal DPCM del 17 febbraio 2017, direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, il cui articolo 8 prevede appunto un « Nucleo per la sicurezza cibernetica », presso il Dipartimento delle informazioni per la sicurezza.

L'articolo 9 determina le funzioni del Nucleo per la cybersicurezza, che: *a)* formula proposte di iniziative in materia di cybersicurezza; *b)* promuove, sulla base delle direttive impartite dal Presidente del Consiglio, la programmazione e la pianificazione operativa, da parte delle amministrazioni e degli operatori privati interessati, della risposta a situazioni di crisi cibernetica, elaborando altresì, in raccordo con le pianificazioni di difesa civile e di protezione civile, le procedure di coordinamento interministeriale; *c)* promuove e coordina lo svolgimento esercitazioni interministeriali – o la partecipazione italiana ad esercitazioni internazionali – di simulazione di eventi di natura cibernetica; *d)* valuta e promuove procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ed in raccordo con le amministrazioni competenti, per specifici profili della cybersicurezza, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi; *e)* 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; *f)* tali comunicazioni giungono dal Dipartimento delle informazioni per la sicurezza (DIS), dalle due Agenzie informazioni e sicurezza, interna ed esterna (AISE e AISI), dalle Forze di polizia, dall'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (previsto dall'articolo 7-*bis* del decreto-legge n. 144 del 2005), dalle strutture del Ministero della difesa, dalle altre amministrazioni che compongono il Nucleo, dai gruppi CERT di intervento per le emergenze informatiche (l'acronimo sta per: *Computer Emergency Response Team*); *g)* riceve dal CSIRT Italia le notifiche di incidente (circa la tassonomia degli incidenti e la loro notifica, richiama, da ultimo, il DPCM n. 81 del 2021); *h)* valuta se le violazioni (o tentativi di violazione) della sicurezza o i casi di perdita dell'integrità significativi o gli incidenti (di cui alle lettere *e)* e *f)*) assumano dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria e da richiedere l'assunzione di decisioni coordinate in sede interministeriale: in tal caso il Nucleo provvede ad informare tempestivamente il Presidente del Consiglio (o l'Autorità delegata, ove istituita) sulla situazione in atto e sullo svolgimento delle attività di gestione della crisi.

L'articolo 10 disciplina le procedure da seguire per la gestione delle crisi che coinvolgono aspetti di cybersicurezza.

In particolare, nelle situazioni di crisi che coinvolgono aspetti di cybersicurezza, il comma 1 prevede che – nei casi in cui il Presidente del Consiglio dei ministri convochi il Comitato interministeriale per la sicurezza della Repubblica (CISR) in materia di gestione delle predette situazioni di crisi – siano chiamati a partecipare alle sedute del Comitato interministeriale: il Ministro delegato per l'innovazione tecno-

logica e la transizione digitale; il direttore generale dell'Agenzia.

In base al comma 2 al Nucleo per la cybersicurezza compete assicurare 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 in base alla previsione in esame, nonché per l'esercizio dei poteri attribuiti al Presidente del Consiglio dei ministri, comprese le attività istruttorie e le procedure di attivazione necessarie, ai sensi dell'articolo 5 del decreto-legge n. 105 del 2019.

Relativamente alla composizione del Nucleo, il comma 3 prevede che in situazioni di crisi di natura cibernetica il Nucleo sia integrato, in ragione della necessità, con un rappresentante, rispettivamente: del Ministero della salute, del Ministero 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.

Tali rappresentanti sono autorizzati ad assumere decisioni che impegnano la propria amministrazione, in base a quanto precisato dal medesimo comma 3. Inoltre, si dispone che alle riunioni i componenti possano farsi accompagnare da altri funzionari della propria amministrazione. Alle medesime riunioni possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anch'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.

In base al comma 4 al Nucleo è affidato il compito, nella composizione per la gestione delle crisi di cui al comma 3, di assicurare che « le attività di reazione e stabilizzazione » di competenza delle diverse amministrazioni ed enti rispetto a situazioni di crisi di natura cibernetica, vengano espletate in maniera coordinata secondo quanto previsto dall'articolo 9, comma 1, lettera *b)*, che attribuisce al Nucleo il compito di promuovere, sulla base delle direttive, la programmazione e pianificazione operativa della risposta a situazioni di crisi cibernetica.

Secondo il comma 5, il Nucleo, per l'espletamento delle proprie funzioni: *a)* mantiene costantemente informato il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla crisi in atto, predisponendo punti aggiornati di situazione; *b)* assicura il coordinamento per l'attuazione a livello interministeriale delle determinazioni del Presidente del Consiglio dei ministri per il superamento della crisi; *c)* raccoglie tutti i dati relativi alla crisi; *d)* elabora rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati; *e)* partecipa ai meccanismi europei di gestione delle crisi cibernetiche, assicurando altresì i collegamenti finalizzati alla gestione della crisi con gli omologhi organismi di altri Stati, della NATO, dell'UE o di organizzazioni internazionali di cui l'Italia fa parte.

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

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

Ai sensi del comma 2, le fonti di finanziamento dell'Agenzia sono rappresentate da: stanziamenti annuali disposti nella legge di bilancio, nell'ambito dell'apposito capitolo istituito dall'articolo 18 del decreto-legge presso lo stato di previsione del Ministero dell'economia: lo stanziamento annuale da assegnare all'Agenzia è stabilito sulla base della determinazione del fabbisogno annuo operata dal Presidente del Consiglio dei ministri e preventivamente comunicata al Copasir; corrispettivi per i servizi prestati a soggetti pubblici o privati; proventi derivanti dallo sfruttamento della proprietà industriale, dei prodotti dell'ingegno e delle invenzioni dell'Agenzia; con-

tribuiti dell'Unione europea o di organismi internazionali, anche derivanti dalla partecipazione a specifici bandi, progetti e programmi di collaborazione; proventi delle sanzioni irrogate dall'Agenzia ai sensi di quanto previsto dal decreto legislativo « NIS », dal decreto-legge « perimetro » e dal decreto legislativo n. 259 del 2003, e relative disposizioni attuative; altri proventi patrimoniali e di gestione e ogni altra eventuale entrata.

A completamento della disciplina, i commi 3 e 4 prevedono l'adozione di due distinti regolamenti, da adottare su proposta del direttore generale dell'Agenzia, secondo la procedura già richiamata. In particolare, ai sensi del comma 3, il regolamento di contabilità dell'Agenzia, volto ad assicurarne l'autonomia gestionale e contabile: tale regolamento può essere adottato anche in deroga alle norme di contabilità generale dello Stato e nel rispetto dei principi fondamentali da quelle stabiliti; tra i principi da rispettare, il regolamento di contabilità deve prevedere che i bilanci dell'Agenzia, preventivo e consuntivo, sono adottati dal direttore generale e approvati con decreto del Presidente del Consiglio dei ministri, previo parere del Comitato interministeriale, nonché trasmessi alla Corte dei conti per il controllo preventivo di legittimità; si dispone inoltre che vengano trasmessi al Copasir il bilancio consuntivo e la relazione della Corte dei conti.

Ai sensi del comma 4, il regolamento che definisce le procedure per la stipula dei contratti di appalti di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, nonché per quelle svolte in raccordo con il Sistema di informazione per la sicurezza di cui alla legge n. 124 del 2007; tale regolamento è adottato anche in deroga alle norme in materia di contratti pubblici, ferma restando la disciplina dei contratti secretati di cui all'articolo 162 del codice di cui al decreto legislativo n. 50 del 2016.

Ai sensi dell'articolo 12 la disciplina del personale addetto all'Agenzia è stabilita in apposito regolamento adottato nel rispetto dei principi generali dell'ordinamento giuridico e dei criteri indicati dal comma 2, anche in deroga alle vigenti disposizioni di legge, ivi incluso il Testo unico delle disposizioni in materia di lavoro alle dipendenze della pubblica amministrazione, adottato con decreto legislativo n. 165 del 2001.

La deroga è posta in correlazione con le funzioni di tutela della sicurezza nazionale nello spazio cibernetico attribuite all'Agenzia e con le attività svolte dall'Agenzia in raccordo con il Sistema di informazione per la sicurezza della Repubblica.

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

La dotazione organica dell'Agenzia, in sede di prima applicazione, è stabilita in un massimo di 300 unità, così ripartite: fino a un massimo di 8 unità di livello dirigenziale generale; fino a un massimo di 24 unità di livello dirigenziale non generale; fino a un massimo di 268 unità di personale non dirigenziale.

Ai sensi del comma 5 tale dotazione organica può essere rideterminata con decreto del Presidente del Consiglio dei ministri, adottato di concerto con il Ministro dell'economia e delle finanze, nei limiti delle risorse finanziarie destinate alle spese per il personale. Dei provvedimenti relativi alla dotazione organica è data tempestiva e motivata comunicazione al presidente del Copasir. A tale riguardo segnala che l'articolo 17, comma 8, del decreto-legge, in relazione alla fase di prima applicazione del decreto e di avvio dell'Agenzia, prevede l'avvalimento di un nucleo di personale, non superiore al 30 per cento della dotazione organica complessiva iniziale, di unità appartenenti ad altre amministrazione.

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

Il comma 7 dispone un obbligo del segreto da parte del personale che presta comunque la propria opera alle dipendenze o in favore dell'Agenzia, su ciò di cui sia venuto a conoscenza nell'esercizio o a causa delle proprie funzioni, anche dopo la cessazione di tale attività. La disposizione fa salve in ogni caso le classifiche di segretezza che, ai sensi dell'articolo 42 della legge n. 124 del 2007, sono attribuite per circoscrivere la conoscenza di informazioni, documenti, atti, attività o cose ai soli soggetti che abbiano necessità di accedervi in ragione delle proprie funzioni istituzionali.

In base al comma 8 i tempi e le modalità di adozione del regolamento sono quelle già evidenziate per gli altri regolamenti di disciplina dell'Agenzia.

Il Ministro Federico D'INCÀ fa presente che seguirà personalmente i lavori sul provvedimento, il quale riveste per il Governo primaria importanza, rilevando come sarà possibile confrontarsi sul testo in particolare nella fase emendativa.

Raffaella PAITA, *presidente*, nessun altro chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta e ricorda che è ora convocata una riunione congiunta degli Uffici di presidenza, integrati dai rappresentanti dei gruppi, delle Commissioni riunite, ai fini dell'organizzazione dell'esame del provvedimento.

La seduta termina alle 14.55.

UFFICIO DI PRESIDENZA INTEGRATO DAI RAPPRESENTANTI DEI GRUPPI

Martedì 22 giugno 2021.

L'ufficio di presidenza si è riunito dalle 14.55 alle 15.