Camera dei deputati
Servizio Studi
XVIII Legislatura

PROVVEDIMENTO D.L. 82/2021 - Disposizioni in materia di sicurezza cibernetica e Agenzia per la cibersicurezza nazionale

6 agosto 2021

Il 3 agosto 2021 il Parlamento ha approvato in via definitiva il disegno di legge di conversione 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. Il testo è stato modificato ed integrato nel corso dell'esame in sede referente delle Commissioni I e IX della Camera. Il 5 agosto il Consiglio dei Ministri ha deliberato su proposta del Presidente Mario Draghi, la nomina del prof. Roberto Baldoni a direttore dell'Agenzia per la cybersicurezza nazionale.

Architettura nazionale di cybersicurezza

I primi 4 articoli del decreto-legge 82/2021 definiscono la *governance* del sistema nazionale di sicurezza cibernetica cha ha al suo vertice il **Presidente del Consiglio dei ministri** cui è attribuita l'**alta direzione e la responsabilità generale** delle "politiche di cybersicurezza", e a cui spetta l'adozione della relativa **strategia nazionale** e la **nomina** dei vertici della nuova **Agenzia per la cybersicurezza nazionale.** Il Presidente del Consiglio dei ministri può **delegare** alla **Autorità delegata per il sistema di informazione per la sicurezza della Repubblica** le funzioni che non sono a lui attribuite in via esclusiva. Presso la Presidenza del Consiglio dei ministri è istituito il **Comitato interministeriale per la cybersicurezza (CIC)**, organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

Nel dettaglio, l'**articolo 1** reca le **definizioni** dei principali termini utilizzati nel decreto. In particolare, viene introdotta la definizione di "**cybersicurezza**", con cui si intende l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini, come specificato dalle Commissioni in sede referente, della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Sempre in sede referente è stata aggiunta la definizione di **"Resilienza nazionale nello spazio cibernetico"** che si riferisce alle attività volte a prevenire un **pregiudizio alla sicurezza nazionale,** ossia un danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale.

Ai sensi dell'**articolo 2** il **Presidente del Consiglio dei ministri** è l'autorità al vertice dell'architettura della sicurezza cibernetica, in quanto è a lui attribuita in **via esclusiva** l'**alta direzione** e la **responsabilità generale** delle politiche di cybersicurezza.

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

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

referente.

Sulle modalità di nomina e revoca dei vertici dell'Agenzia sono intervenute le Commissioni **in sede referente**, prevedendo che il Presidente del Consiglio **informi** preventivamente circa le nomine il **COPASIR** (il decreto-legge nel testo iniziale, poi modificato in sede referente, faceva riferimento al Presidente del COPASIR). Inoltre, si prevede l'invio della comunicazione anche alle **Commissioni parlamentari competenti**.

La disposizione in esame non interviene sui contenuti della strategia nazionale di sicurezza cibernetica, che rimangono disciplinati dal D.Lgs. 65/2018, ma ne muta la denominazione in strategia nazionale di cybersicurezza e provvede a modificare la procedura di adozione prevedendo il parere del nuovo Comitato interministeriale per la cybersicurezza anziché del CISR.

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

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

L'Autorità delegata è tenuta a **informare costantemente** il Presidente del Consiglio sulle modalità di esercizio delle funzioni delegate, il quale, "fermo restando il potere di direttiva" può in qualsiasi momento avocare a sé l'esercizio di tutte o di alcune di esse.Con il D.P.C.M. 13 settembre 2021 è stata conferita la delega di funzioni in materia di cybersicurezza all'Autorità delegata per la sicurezza della Repubblica, prefetto Franco Gabrielli.

L'Autorità delegata, in relazione alle funzioni delegate, partecipa alle riunioni del **Comitato interministeriale per la transizione digitale** istituito dal D.L. 22/2021, quale sede di **coordinamento** e **monitoraggio** dell'attuazione delle **iniziative di innovazione tecnologica e transizione digitale** delle pubbliche amministrazioni.

L'**articolo 4** completa l'assetto di *governance* della nuova Architettura nazionale di cybersicurezza e della 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,

Il Comitato è composto come segue:

- il Presidente del Consiglio (che lo presiede);
- l'Autorità delegata, ove istituita;
- il Ministro degli affari esteri e della cooperazione internazionale;
- il Ministro dell'interno;
- il Ministro della giustizia;
- il Ministro della difesa;
- il Ministro dell'economia e delle finanze;
- il Ministro dello sviluppo economico;
- il Ministro della transizione ecologica;
- il Ministro dell'università e della ricerca;
- il Ministro delegato per l'innovazione tecnologica e la transizione digitale;
- il Ministro delle infrastrutture e della mobilità sostenibili.

Al CIC sono attribuiti 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.

Inoltre, vengono 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.

Dossier

Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale
https://temi.camera.it/dossier/OCD18-15441/disposizioni-urgenti-materia-cybersicurezza-definizione-architettura-nazionale-cybersicurezza-e-istituzione-agenzia-cybersicurezza.html

---

Agenzia per la cybersicurezza nazionale

Il decreto, all'articolo 5, prevede **l'istituzione dell'Agenzia per la cybersicurezza nazionale** a tutela degli interessi nazionali nel campo della cybersicurezza. L'istituzione dell'Agenzia è strumentale all'esercizio delle competenze che il decreto-legge assegna al Presidente del Consiglio dei ministri e all'Autorità delegata, ove istituita.

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

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

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

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

Tutti i regolamenti sono adottati, **entro centoventi giorni** dalla data di entrata in vigore della legge di conversione del decreto in esame, con **decreto del Presidente del Consiglio dei ministri**, anche in deroga alle previsioni dell'articolo 17 della legge 23 agosto 1988, n. 400. Tutti i regolamenti sono adottati **previo parere del Copasir**, sentito il **Comitato interministeriale** per la cybersicurezza; inoltre, come previsto nel corso dell'esame in sede referente, sugli schemi di regolamento di organizzazione e funzionamento dell'Agenzia (art. 6, co. 3) e di regolamento del personale dell'Agenzia (art. 12, co. 8) è richiesto il **parere delle Commissioni parlamentari competenti, anche per i profili finanziari.** Inoltre, è stato specificato che il parere del **Copasir** è espresso **per i profili di competenza**.

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

Per quanto riguarda l'**organizzazione dell'Agenzia**, che ha la sede principale in Roma, il decreto (art. 6) prevede i seguenti organi:

- il **direttore generale,** che rappresenta l'organo di gestione ed 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 per un massimo di ulteriori 4 anni;
- il **collegio dei revisori dei conti**, quale organo di controllo interno, per la cui composizione ed il funzionamento si fa rinvio interamente al regolamento.

L'Agenzia è articolata in uffici di livello dirigenziale generale, che il decreto stabilisce nel numero massimo di otto e in uffici di livello dirigenziale non generale, fino ad un massimo di trenta.

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

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

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

- il **regolamento di contabilità dell'Agenzia**, volto ad assicurarne l'autonomia gestionale e contabile (art. 11, comma 3). Tale regolamento può essere adottato anche **in deroga alle norme di contabilità** generale dello Stato e nel rispetto dei principi fondamentali da quelle stabiliti. Tra i principi da rispettare, il regolamento di contabilità deve prevedere che i **bilanci dell'Agenzia**, preventivo e consuntivo, sono adottati dal direttore generale e approvati con dPCm, previo parere del Comitato interministeriale, nonché trasmessi alla Corte dei conti per il controllo preventivo di legittimità. Si dispone inoltre che vengano trasmessi al **Copasir** e, come aggiunto in sede referente, alle **Commissioni parlamentari competenti**, il bilancio consuntivo e la relazione della Corte dei conti;
- il **regolamento** (art. 11, comma 4) che definisce le procedure per la stipula dei **contratti di appalti** di lavori e forniture di beni e servizi per le attività dell'Agenzia finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, e in materia di contratti pubblici, ferma restando la disciplina dei contratti secretati di cui all'art. 162 del Codice di cui al D.Lgs. n. 50 del 2016.

La **disciplina del personale** addetto all'Agenzia, di cui all'articolo 12 del decreto, è stabilita in apposito **regolamento** adottato **nel rispetto dei principi generali dell'ordinamento giuridico** e dei criteri indicati nel decreto , anche **in deroga alle vigenti disposizioni di legge**, ivi incluso il Testo unico delle disposizioni in materia di lavoro alle dipendenze della PA, adottato con D.Lgs. n. 165 del 2001. In proposito, il Decreto stabilisce

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

Il regolamento del personale determina in particolare (comma 2) l'istituzione di un **ruolo del personale dell'Agenzia** e la disciplina generale del rapporto d'impiego. Al contempo si prevede 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". L'assunzione a tempo determinato deve risultare necessaria per lo svolgimento di attività assolutamente necessarie all'operatività dell'Agenzia o per specifiche progettualità da portare a termine in un arco di tempo prefissato. è prevista infine la possibilità di avvalersi di un contingente di **esperti**, non superiore a cinquanta unità, composto da personale proveniente da pubbliche amministrazioni ovvero da personale non appartenente alla PA, in possesso di specifici requisiti di competenza e di esperienza indicati dalla norma, nonchè la possibilità di impiegare **personale del Ministero della difesa**, secondo termini e modalità che dovranno essere definite con apposito dPCm.

La **dotazione organica** dell'Agenzia, in sede di prima applicazione, è stabilita dal decreto in un **massimo di 300 unità.**

Infine, si dispone un obbligo del segreto da parte del personale che presta comunque la propria opera alle dipendenze o in favore dell'Agenzia al rispetto del segreto su ciò di cui sia venuto a conoscenza nell'esercizio o a causa delle proprie funzioni, anche dopo la cessazione di tale attività.

Le funzioni e i compiti dell'Agenzia

All'Agenzia per la cybersicurezza nazionale, istituita dal decreto-legge n. 82 del 2021 e qualificata quale **Autorità nazionale** ai fini del complesso di relazioni e funzioni disegnato dalle norme europee ed interne, incluse quelle di certificazione della cibersicurezza, sono attribuite le **funzioni i**ndividuate in primo luogo dall'articolo 7, come risultante dalle modifiche apportate in sede referente.

All'Agenzia spetta in particolare predisporre la strategia nazionale di cibersicurezza; assumere 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; promuovere iniziative per lo sviluppo di competenze e capacità.

Presso l'Agenzia sono inoltre trasferiti il *Computer Security Incident Response Team*-CSIRT italiano - ora CSIRT Italia - e il Centro di valutazione e certificazione nazionale (CVCN).

Come previsto in sede referente l'Agenzia inoltre assume le iniziative idonee a valorizzare la crittografia come strumento di cibersicurezza, provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione, promuove iniziative di partenariato pubblico-privato, onde rendere effettive le capacità di prevenzione e rilevamento e risposta ad incidenti ed attacchi informatici, sostiene negli ambiti di competenza lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche, assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisca competenze in materia di cibersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare.

L'Agenzia può altresì promuovere la costituzione di "aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cibersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzate a tale scopo", assicurando il raccordo con le altre amministrazioni a cui la legge attribuisca competenze in materia di cibersicurezza.e in particolare con il **Ministero della difesa** per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia Europea per la Difesa.

È inoltre prevista **l'istituzione di un Comitato tecnico-scientifico**, presso l'Agenzia, con funzioni di **consulenza e di proposta**. Tale Comitato è presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, ed è composto da personale della stessa Agenzia nonché da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri.

Disposizioni per la prima operatività dell'Agenzia

Per assicurare la prima operatività dell'Agenzia, il decreto (art. 17) demanda ad uno o più decreti del

Presidente del Consiglio dei ministri, da adottarsi entro centottanta giorni dall'entrata in vigore del decreto-legge, la definizione di termini e di modalità, onde trasferire funzioni, beni strumentali e documentazione, attuare le disposizioni del decreto-legge, regolare le riduzioni di risorse finanziarie relative alle amministrazioni cedenti. Con d.P.C.m. è altresì definito il dovuto raccordo tra la neo-istituita Agenzia e l'Agenzia per l'Italia digitale (AgID), per quanto concerne il trasferimento di funzioni da questa a quella.

Per garantire l'organico necessario all'avvio dell'Agenzia, si prevede in primo luogo che il **Dipartimento delle informazioni per la sicurezza (DIS)** metta a disposizione il **personale** impiegato nell'ambito delle attività relative allo svolgimento delle funzioni oggetto di trasferimento. Inoltre si stabilisce che per un periodo massimo di sei mesi - prorogabile una sola volta, per un massimo di ulteriori sei mesi – l'Agenzia si **avvalga di personale appartenente** al Ministero dello sviluppo economico, all'Agenzia per l'Italia digitale, **ad altre pubbliche amministrazioni** e ad autorità indipendenti, messo a disposizione dell'Agenzia stessa su specifica richiesta e secondo modalità individuate mediante intese. Numericamente, il personale esterno temporaneamente a disposizione dell'Agenzia **non può eccedere il 30 per cento** della dotazione organica complessiva iniziale dell'Agenzia stessa.

Il personale di primo avvalimento o il personale assunto a **tempo determinato** potrà essere inquadrato attraverso modalità selettive, nella misura massima del **50 per cento** della dotazione organica complessiva dell'Agenzia.

Nucleo per la cybersicurezza e gestione delle crisi

E' prevista la costituzione, presso l'Agenzia, di un **Nucleo per la cybersicurezza (articolo 8).**

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

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

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

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

I componenti possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni, in relazione alle materie oggetto di trattazione.

In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di **altre amministrazioni**, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza.

A fronte di questa composizione 'allargata', è prevista una possibile composizione 'ristretta', con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi.

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

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

Tra le funzioni poste in capo al Nucleo sono previste dall'articolo 9 quelle di:

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

b) promuovere (sulla base delle direttive del 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**. Altresì elabora, in raccordo con le pianificazioni di difesa civile e di protezione civile, le procedure di coordinamento interministeriale. La disposizione mantiene fermo l'articolo

7-*bis*, comma 5, del decreto-legge n. 174 del 2015, secondo cui il Comitato interministeriale per la sicurezza della Repubblica può essere convocato dal Presidente del Consiglio dei ministri, con funzioni di consulenza, proposta e deliberazione, in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale;

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

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

e) secondo quanto specificato nel corso dell'esame in **sede referente** acquisire, anche 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 del servizi dagli organismi di informazione DIS, AISE e AISI , dalle Forze di polizia, dall'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, dalle strutture del Ministero della difesa, dalle altre amministrazioni che compongono il Nucleo, dai gruppi CERT di intervento per le emergenze informatiche (l'acronimo sta per: *Computer Emergency Response Team*);

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

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

Trattamento dei dati personali

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

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

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

Relazioni al Parlamento

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

La prima relazione al Parlamento deve essere trasmessa, come specificato in sede referente all'art. 17, entro il **30 novembre 2022**.

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

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

Modifiche alla legislazione vigente

Il decreto-legge n. 82 del 2021 - agli articoli 15 e 16 - reca una serie di modifiche alla normativa vigente al fine di adeguarla alla nuova architettura delineata. Sono in particolare oggetto di modifica il d. lgs. 65 del

2018 che ha dato attuazione alla c.d. direttiva NIS, il decreto-legge n. 105 del 2019 che ha, in particolare, istituito il perimetro di sicurezza cibernetica e la legge n. 124 del 2007, che reca la disciplina del Sistema di informazione per la sicurezza della Repubblica, per le parti in cui sono previste diverse attribuzioni di competenza.

Modifiche al D.Lgs. 65/2018 di attuazione della direttiva NIS

E' in primo luogo oggetto di modifica (dall'art. 15) il decreto legislativo n. 65 del 2018 che ha dato attuazione alla direttiva (UE) 2016/1148 ***(c.d.*** **direttiva** ***Network and Information Security*** - NIS).

Tale decreto legislativo rappresenta la cornice legislativa delle misure per la sicurezza delle reti e dei sistemi informativi e dei soggetti competenti a dare attuazione agli obblighi previsti in tale ambito.

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

Le modifiche recate dall'art. 15 sono volte ad **adeguare il decreto legislativo n. 65 del 2018** alle previsioni del **decreto-legge 82/2021**.

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

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

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

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

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

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

Viene specificato che l'autorità nazionale competente NIS è **responsabile dell'attuazione** delle misure previste dal decreto legislativo n. 65/2018 con riguardo ai settori e servizi ivi elencati (allegato II e allegato III) e ad essa spetta la **vigilanza** sull'applicazione del decreto a livello nazionale, incluso l'esercizio delle relative **potestà ispettive e sanzionatorie**

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

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

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

Ai sensi del nuovo art. 9 del D.Lgs. N. 65/2018 le autorità di settore collaborano con l'autorità nazionale

competente NIS per l'adempimento degli obblighi di al medesimo decreto. A tal fine il **Comitato tecnico di raccordo** opera **presso l'Agenzia** per la cybersicurezza nazionale, anziché presso la Presidenza del Consiglio dei ministri.

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

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

Per quanto riguarda le procedure di **notifica** degli incidenti, di cui all'art. 14 del d.lgs, 65/2018, si prevede che i fornitori di servizi digitali **notifichino al CSIRT italiano** (e non più, per conoscenza, all'autorità competente NIS) senza ingiustificato ritardo, **gli incidenti** aventi un impatto rilevante sulla fornitura di un servizio (di cui all'allegato III del decreto n. 65) che essi offrono all'interno dell'Unione europea.

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

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

Modifiche alla L. 124/2007

Viene modificato in primo luogo (dall'art. 16 del decreto-legge) l'articolo 3, comma 1-*bis* della legge 124/2007 che, nel testo previgente, non consente all'Autorità delegata di esercitare **funzioni** di governo **ulteriori** rispetto a quelle ad essa delegate dal Presidente del Consiglio dei ministri nell'ambito del sistema di informazioni per la sicurezza della Repubblica a norma della medesima legge 124. Con il comma in esame si consente all'Autorità delegata di svolgere anche le funzioni "in materia di cybersicurezza". La modifica è posta in relazione con l'articolo 3 del decreto in esame che dà facoltà al Presidente del Consiglio di delegare le competenze in materia di cibersicurezza alla medesima Autorità delegata per la sicurezza della Repubblica, se istituita.

Viene abrogato il comma 1-*bis* dell'articolo 38 della legge 124/2007, a decorrere **dal 1° gennaio 2023**, come specificato nel corso dell'**esame in sede referente**. Tale disposizione prevede che alla relazione annuale sulla **politica dell'informazione** per la sicurezza e sui risultati ottenuti (da trasmettere al Parlamento entro il mese di febbraio), sia allegato il **documento di sicurezza nazionale**, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica.

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

La denominazione **CSIRT Italia** (*Computer Security Incident Response Team*) sostituisce, ovunque presente, quella di CSIRT Italiano.

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

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

- le parole: «Comitato interministeriale per la sicurezza della Repubblica (CISR)» e «CISR», ovunque ricorrano, sono rispettivamente sostituite dalle seguenti: «Comitato interministeriale per la cybersicurezza (CIC)» e «CIC», ad eccezione per le disposizioni di cui all'articolo 5 del medesimo decreto-legge;
- i riferimenti al Dipartimento delle informazioni per la sicurezza, o al DIS, ovunque ricorra, sono da intendersi riferiti all'Agenzia per la cybersicurezza nazionale e i riferimenti al Nucleo per la sicurezza cibernetica sono da intendersi riferito al Nucleo per la cybersicurezza;
- i riferimenti al Ministero dello sviluppo economico e alla Presidenza del Consiglio dei ministri, ovunque

ricorrano, sono da intendersi riferito all'Agenzia per la cybersicurezza nazionale;

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

Infine, nei provvedimenti attuativi di natura regolamentare e amministrativa previsti dall'articolo 1 del medesimo DL 105/2019, i riferimenti al CISR e al DIS sono da intendersi al CIC e all'Agenzia per la cybersicurezza nazionale.

Modifiche al decreto-legge n. 105 del 2019 sul perimetro nazionale

Alcune disposizioni infine (articolo 16, commi 8-14) modificando il decreto-legge n. 105 del 2019 volte ad adeguare le disposizioni del citato decreto-legge alle modifiche intervenute e a rendere più fluide, a seguito di modifiche introdotte in sede referente, le comunicazioni tra i vari soggetti responsabili per la cybersicurezza.

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

Sono inserite inoltre tra gli ambiti di competenza del **TAR del Lazio, sede di Roma**, le controversie aventi ad oggetto i provvedimenti dell'Agenzia per la cybersicurezza nazionale nonchè, come specificato in sede referente, quelle sul rapporto di lavoro del personale dell'Agenzia.

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