Camera dei deputati
Servizio Studi
XVIII Legislatura

Sicurezza cibernetica

22 maggio 2022

Il Governo ha trasmesso al Parlamento uno schema di decreto legislativo volto all'adeguamento della normativa nazionale alle disposizioni dell'Unione europea relative alla certificazione della cibersicurezza dei prodotti, dei servizi e dei processi relativi alle tecnologie dell'informazione e della comunicazione (ICT).

In considerazione dell'accresciuta esposizione alle minacce cibernetiche si è imposta nell'agenda nazionale ed internazionale la necessità di sviluppare, in tempi brevi, idonei e sempre più stringenti meccanismi di tutela.

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

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

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

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

Infine, con il decreto-legge 14 giugno 2021, n. 82, si è proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale.

La sicurezza cibernetica nel PNRR e l'istituzione dell'Agenzia per la cybersicurezza nazionale

La sicurezza cibernetica è compresa tra i progetti finanziati dal Piano nazionale di ripresa e resilienza (PNRR).

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

All'investimento, volto alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese a partire dalla attuazione della disciplina prevista dal perimetro di sicurezza nazionale cibernetica, sono destinati ca. **620 milioni di euro** di cui 241 per la creazione di una infrastruttura per la cybersicurezza; 231 per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica PNSC; 15 per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'Interno, Difesa, Guardia di Finanza, Giustizia e Consiglio di Stato.

L'intervento si articola in 4 aree principali:

- rafforzamento dei **presidi di *front-line*** per la gestione degli *alert* e degli eventi a rischio verso la PA e le imprese di interesse nazionale;
- consolidamento delle capacità tecniche di **valutazione e audit della sicurezza** dell'*hardware* e del *software*;
- potenziamento del **personale delle forze di polizia** dedicate alla prevenzione e investigazione del crimine informatico;
- implementazione degli asset e delle unità incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber.

Il Piano prevede, tra l'altro, l'individuazione di un nuovo organismo per la sicurezza informatica nazionale per guidare l'architettura nazionale generale della cibersicurezza: "Nell'ambito delle capacità previste, tale autorità contribuirebbe alla creazione di programmi di accelerazione per le PMI e le start-up in materia di cibersicurezza, alla direzione delle pertinenti attività di ricerca e all'individuazione del punto di contatto nazionale con le controparti europee pertinenti nell'ambito dello scudo informatico dell'UE (ad esempio, la rete e i centri di competenza in materia di cibersicurezza e i centri di condivisione e analisi delle informazioni)".

Anche alla luce di tali previsioni con il decreto-legge n. 82 del 2021 è stata definita 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 cibersicurezza 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. L'**Agenzia per la cybersicurezza nazionale (ACN)** è istituita a tutela degli interessi nazionali nel campo della cibersicurezza. L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria.

L'Agenzia è l'Autorità nazionale per la cybersicurezza e in quanto tale ha il **coordinamento** tra i soggetti pubblici coinvolti nella cibersicurezza a livello nazionale. Promuove azioni comuni dirette ad assicurare la sicurezza cibernetica, a sviluppare la digitalizzazione del sistema produttivo e delle pubbliche amministrazioni e del Paese, nonché a conseguire autonomia (nazionale ed europea) per i prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore. Essa predispone la **strategia nazionale di cibersicurezza**.

Ai sensi del nuovo Codice europeo delle comunicazioni elettroniche, svolge anche i compiti relativi alla **sicurezza delle reti e dei servizi di comunicazione elettronica** accessibili al pubblico e alla protezione dalle minacce informatiche delle comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone altresì la resilienza (D.Lgs. 8 novembre 2021, n. 207, art. 6, comma 3 e artt. 40 e 41).

Il decreto-legge prevede l'adozione dei seguenti provvedimenti attuativi:

- regolamento di organizzazione e funzionamento (art. 6, comma 3), adottato con il DPCM 9 dicembre 2021, n. 223;
- regolamento di contabilità (art. 11, comma 3), adottato con il DPCM 9 dicembre 2021, n. 222;
- regolamento sulle procedure per la stipula di contratti di appalti di lavori e forniture per le attività finalizzate alla sicurezza (art. 11, comma 4);
- regolamento del personale (art. 12, comma 8), adottato con il DPCM 9 dicembre 2021, n. 224;
- provvedimenti recante i termini e le modalità del trasferimento di funzioni, beni strumentali e documentazione alla ACN (art.17, comma 5): DPCM 16 settembre 2021 per il traferimento dal Dipartimento delle informazioni per la sicurezza; DPCM 15 giugno 2022 per il trasferimento dal Ministero dello sviluppo economico.

Il Consiglio dei Ministri, nella seduta del 5 agosto 2021, ha deliberato su proposta del Presidente Mario Draghi, la nomina del prof. Roberto Baldoni a direttore dell'Agenzia per la cybersicurezza nazionale. Nella

seduta del 16 settembre 2021 è stata deliberata la nomina della dottoressa Annunziata Ciardi quale Vice direttore generale dell'Agenzia per la cybersicurezza nazionale.

Il 15 giugno 2022 il Sottosegretario di Stato alla Presidenza del Consiglio Gabrielli, Autorità delegata per la sicurezza della Repubblica, ha nominato i 9 membri el Comitato tecnico scientifico dell'Agenzia per la cybersicurezza nazionale.

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/OCD18-15472/disposizioni-urgenti-materia-cybersicurezza-definizione-architettura-nazionale-cybersicurezza-e-istituzione-agenzia-cybersicurezza.html

Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale
https://temi.camera.it/dossier/OCD18-15865/regolamento-organizzazione-e-funzionamento-agenzia-cybersicurezza-nazionale-1.html

Schema di decreto del Presidente del Consiglio dei ministri recante regolamento del personale dell'Agenzia per la cybersicurezza nazionale
https://temi.camera.it/dossier/OCD18-15866/schema-decreto-del-presidente-del-consiglio-ministri-recante-regolamento-del-personale-agenzia-cybersicurezza-nazionale-1.html

I rischi connessi all'accresciuta esposizione alle minacce di tipo cibernetico

A seguito della crisi in Ucraina sono state adottate alcuni disposizioni di urgenza finalizzate alla **diversificazione delle dotazioni informatiche delle pubbliche amministrazioni** (D.L. 21/2022, art. 29).

Si prevede le pubbliche amministrazioni provvedano alla **diversificazione dei prodotti informatici in uso**, al fine di prevenire pregiudizi alla **sicurezza delle reti, dei sistemi informativi e dei servizi informatici**. Si tratta dei rischi legati all'eventualità che le aziende produttrici di tali prodotti informatici, legate alla Federazione Russa, non siano in grado di fornire servizi e aggiornamenti atti a prevenire i rischi medesimi, a seguito della crisi in Ucraina anche al fine di prevenire possibili pregiudizi per la sicurezza nazionale nello spazio cibernetico.

Inoltre, si demanda ad una **circolare** dell'Agenzia per la cybersicurezza nazionale l'individuazione delle **categorie di prodotti** destinate alla sicurezza dei dispositivi (antivirus, antimalware, EDR) ovvero alla protezione delle reti (*firewall*). Nella circolare sono indicate, altresì, le principali raccomandazioni procedurali (ferma restando la responsabilità di ciascuna amministrazione) nonché le categorie di prodotti e servizi, ivi incluse le relative aziende produttrici o fornitrici. In attuazione di tale disposizione, l'Agenzia per la cybersicurezza nazionale ha emanato la circolare 21 aprile 2022, n. 4336, relativa alla "Diversificazione di prodotti e servizi tecnologici di sicurezza informatica".

Nelle Relazioni sulla politica dell'informazione trasmesse al Parlamento (quale la Relazione annuale al Parlamento e il Documento di sicurezza nazionale) si pone in evidenza il rilevante impatto che hanno avuto – sulla vita dei singoli, così come sugli equilibri politico-economici e sullo stesso modo di "giocare la partita democratica" – la rapida, massiva **diffusione delle nuove tecnologie** e la conseguente, istantanea fruibilità a livello globale di notizie e dati, e quindi di conoscenza, ma anche di rappresentazioni mistificate o tout court infondate e di narrazioni distorte o falsificate.

Viene ricordato come negli ultimi anni il **dominio cibernetico** ha continuato a costituire spazio privilegiato per attività ostili, di diversa matrice, condotte in danno di target nazionali – tanto pubblici che privati, con differente livello di strutturazione, a partire dal singolo individuo fino ad arrivare alla più complessa organizzazione istituzionale o aziendale – la cui esposizione alla minaccia è riconducibile alla crescente pervasività degli strumenti di comunicazione elettronica e di digitalizzazione delle informazioni e dei processi. La continua evoluzione del dominio cibernetico, quindi, nell'ampliare la superficie di attacco, ha parallelamente comportato una pronunciata diversificazione ed un **affinamento dei vettori della minaccia**.

Tattiche, tecniche e procedure si sono caratterizzate, infatti, per diversi livelli di capacità offensiva: dalla negazione di servizio alla violazione di sistemi ICT, attraverso operazioni, spesso silenti, finalizzate a compromettere risorse di cui assumere il controllo, così da acquisire i dati in esse contenute.

Parallelamente ha assunto rilievo crescente il **cyber terrorismo**, con implementazioni di *webstrategies* per mantenere una certa visibilità, funzionale a proseguire, sul piano virtuale, l'opera di proselitismo, radicalizzazione e reclutamento di nuove leve.

Lo **strumento cibernetico** – viene evidenziato nelle Relazioni annualmente trasmesse alle Camere – è destinato a divenire sempre di più un agevolatore di attività di influenza, realizzate attraverso la manipolazione e la diffusione mirata di informazioni preventivamente acquisite attraverso manovre intrusive nel cyber-spazio, così da orientare le opinioni pubbliche, fomentare le tensioni socio-economiche, accrescere l'instabilità politica dei Paesi dell'area occidentale, all'atto dell'adozione di decisioni strategiche, ritenute dall'attore ostile sfavorevoli ai propri interessi.

Come evidenziato dal **Parlamento europeo** il tema della cybercicurezza sarà prioritario nei prossimi anni: gli attacchi informatici e la criminalità informatica stanno aumentando in tutta Europa sia in termini di quantità che di sofisticazione, una tendenza destinata a crescere in futuro, considerato che nel 2025 si prevedono oltre 25 miliardi di apparecchi connessi. Nel 2019 il numero degli attacchi riportati è triplicato con circa 700 milioni di ciberattacchi. Il costo annuale del cibercrimine nel 2020 è stato stimato in 5500 miliardi, il doppio rispetto al 2015. nel portare avanti la transizione digitale, rafforzando e-goverment e digitalizzazione della giustizia, il PE ricorda che è indispensabile puntare su alti livelli di cybersicurezza. Quindi l'UE, sulla base dell'EU Cybersecurity Act, punta a raggiungere un elevato livello di sicurezza in tutti i Paesi europei attraverso innovazione, cooperazione e sostegno agli attori pubblici e privati.

Nel dicembre 2020 la **Commissione Ue** ha presentato inoltre la nuova strategia per la cybersicurezza come componente essenziale della transizione digitale, del piano per la ripresa europea e della strategia per l'Unione della sicurezza.

Contestualmente, la Commissione ha presentato proposte di direttiva sulla resilienza informatica e fisica delle entità e delle reti critiche. Le nuove iniziative strategiche comprendono: un cyberscudo europeo composto da centri operativi di sicurezza; un'unità congiunta per il ciberspazio che riunisca tutte le comunità operanti nel settore; soluzioni europee per rafforzare la sicurezza di Internet a livello mondiale; un regolamento per garantire un'Internet delle cose sicure; un pacchetto di strumenti per la diplomazia informatica; una cooperazione rafforzata nell'ambito della cyberdifesa; un programma d'azione ONU in materia di sicurezza internazionale nel ciberspazio; dialoghi informatici con i paesi terzi e con la NATO; un'agenda UE per lo sviluppo delle capacità informatiche esterne.

Il Parlamento europeo ha approvato programmi specifici, come Digital Europe, che stanza 1.7 miliardi per questo settore, prevendendo la realizzazione di un centro di competenza a Bucarest.

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

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

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

La direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo **n. 65** del 18 maggio 2018.

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

In particolare, al **Presidente del Consiglio dei ministri** compete l'adozione, sentito il Comitato interministeriale per la sicurezza della Repubblica (**CISR**), della strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale. Con la medesima procedura sono adottate linee di indirizzo per l'attuazione della strategia nazionale di sicurezza cibernetica.

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

Presso la Presidenza del Consiglio dei ministri è istituito il **CSIRT-***Computer Emergency Response Team* italiano, con un contingente di 30 persone e lo stanziamento di specifiche risorse finanziarie, al quale sono attribuite – a decorrere dall'entrata in vigore del relativo decreto di organizzazione e funzionamento - le funzioni del CERT nazionale (attualmente presso il Ministero per lo sviluppo economico) e del CERT-PA (attualmente presso l'Agenzia per l'Italia digitale-AGID). Il CSIRT è definito dalla direttiva 2016/1148 quale "gruppo di intervento per la sicurezza informatica in caso di incidente", che ogni Stato membro è chiamato a designare con il compito di trattare gli incidenti e i rischi secondo una procedura definita.

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

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

Gli **operatori di servizi essenziali**, ai fini del provvedimento, sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), individuati dalle autorità competenti NIS. Entro il 9 novembre 2018 le autorità competenti sono tenute ad identificare tali soggetti, ai fini del rispetto degli obblighi della direttiva.

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

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

La definizione del perimetro di sicurezza cibernetica

Il **decreto-legge n. 105 del 2019** è stato adottato al fine di assicurare, in particolare, un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari *standard* di sicurezza rivolti a minimizzare i rischi.

Con tale provvedimento sono state quindi dettate modalità e procedure per l'istituzione del perimetro di sicurezza nazionale cibernetica, volto ad assicurare la sicurezza di reti, sistemi informativi e servizi informatici necessari allo svolgimento di funzioni o alla prestazione di servizi, dalla cui discontinuità possa derivare un pregiudizio alla sicurezza nazionale. Si interviene inoltre sulle **procedure, modalità e termini** ai quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici individuati nell'elenco trasmesso alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico.

Sono poi individuati alcuni **compiti** del Centro di valutazione e certificazione nazionale (**CVCN**), con riferimento all'**approvvigionamento** di prodotti, processi, servizi di tecnologie dell'informazione e della comunicazione (ICT) e associate infrastrutture - qualora destinati a reti, sistemi informativi, sistemi informatici ricompresi nel perimetro di sicurezza nazionale cibernetica.

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

È altresì previsto che il Presidente del Consiglio - su deliberazione del CISR - possa disporre la **disattivazione**, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati. Entro 30 giorni il Presidente del Consiglio è tenuto a informare il Comitato parlamentare per la sicurezza della Repubblica (Copasir) delle misure disposte.

Al Presidente del Consiglio dei ministri è affidato inoltre il coordinamento della coerente attuazione delle disposizioni del decreto-legge che disciplinano il perimetro di sicurezza nazionale cibernetica, anche avvalendosi del DIS che assicura gli opportuni raccordi con le autorità titolari delle attribuzioni e con i soggetti coinvolti.

Il Presidente del Consiglio dei ministri **trasmette alle Camere una relazione** sulle attività svolte dopo l'adozione degli atti normativi secondari previsti per l'attuazione delle misure ivi stabilite.

E' stata infine disposta l'istituzione di un Centro di valutazione (CEVA) presso il Ministero dell'interno il quale, come quello del Ministero della difesa, sono accreditati presso il Centro di Valutazione e certificazione nazionale (CVCN) e sono tenuti ad impiegare metodologie di verifica e test quali definiti dal medesimo CVCN. Con DPCM saranno inoltre definiti gli obblighi di informativa di tali Centri con il CVCN.

Il provvedimento reca quindi un articolato **sistema sanzionatorio** per i casi di violazione degli obblighi ivi previsti ed individua le **autorità competenti** all'accertamento delle violazioni e all'irrogazione delle **sanzioni.**

Successivamente, il **decreto-legge n. 162 del 2019**, recante proroga di termini e ulteriori disposizioni in materia di p.a., ha apportato (art. 27) alcune modifiche all'articolo 1 del decreto-legge n. 105 del 2019 in materia di sicurezza nazionale cibernetica, con particolare riguardo alle procedure e alle modalità per la definizione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica.

In particolare, la determinazione puntuale dei soggetti inclusi nel perimetro è stata affidata ad un atto amministrativo del Presidente del Consiglio dei ministri anziché ad un DPCM, come originariamente previsto dal decreto-legge n. 105, al quale spetta invece la determinazione delle modalità e dei criteri procedurali per la relativa individuazione. Ciò in ragione del fatto che "l'elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, considerato nella sua interezza, presenta particolari profili di sensibilità sotto il profilo della sicurezza".

In attuazione di tale disposizione il Governo ha adottato il DPCM 30 luglio 2020, n. 131 (G.U. 21 ottobre 2020, n. 261) che provvede a:

- definire le modalità e i criteri procedurali di individuazione dei soggetti (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, sono tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge 105/2019;
- definire i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica.

Inoltre, il medesimo decreto-legge 162 (all'art. 26) ha previsto che il *Computer security incident response team* – CSIRT italiano, istituito presso la Presidenza del Consiglio, sia incardinato nel Dipartimento delle informazioni per la sicurezza – DIS, in aderenza con il decreto del Presidente del Consiglio dell'8 agosto 2019 che ha previsto la costituzione del CSIRT presso il DIS.

E' stata, inoltre, disposta l'istituzione della **Direzione generale per lo sviluppo della prevenzione e tutela informatiche** presso il Dipartimento della pubblica sicurezza del Ministero dell'interno ad opera del decreto-legge 34/2020 (cd. decreto Rilancio, art. 240).

A tale direzione generale sono attribuiti:

- **lo sviluppo della prevenzione e tutela informatica e cibernetica** (quale struttura per la sicurezza e per la regolarità dei servizi di telecomunicazione, preposta ad assicurare i servizi di protezione

informatica ed i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate;

- lo sviluppo delle attività attribuite al Ministero dell'interno in materia di **perimetro di sicurezza nazionale cibernetica**;
- l'unità di indirizzo e **coordinamento delle attività svolte dalla polizia postale e delle comunicazioni**, specialità della Polizia di Stato - e degli altri compiti che costituiscano il completamento di supporto alle attività investigative.

In attuazione di tale disposizione il Governo ha trasmesso alle Camere lo schema di decreto del Presidente della Repubblica concernente regolamento recante modifiche al regolamento di organizzazione degli uffici centrali di livello dirigenziale generale del Ministero dell'interno, che, tra l'altro disciplina la nuova **Direzione centrale per la polizia scientifica e la sicurezza cibernetica** (A.G. 301).

In attuazione del decreto-legge n. 105 sono stati definiti inoltre seguenti provvedimenti:

- DPR 5 febbraio 2021, n. 54, che ha definito le procedure e modalità di valutazione delle acquisizioni da parte dei soggetti inclusi nel perimetro di sicurezza cibernetica, di oggetti di fornitura le procedure delle attività di verifica e ispezione (art. 1, comma 6, DL 105/2019);
- DPR 14 aprile 2021, n. 81 che definisce le modalità per la notifica nel caso di incidenti riguardanti beni ITC (art. 1, comma 2, lett. b), DL 105/2019);
- DPCM 15 giugno 2021 che individua le categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica (art. 1, comma 6, lett. a) DL 105/2019;
- DPCM 18 maggio 2022, n. 92 in materia di accreditamento dei laboratori di prova e di raccordi tra Centro di Valutazione e Certificazione Nazionale, i laboratori di prova accreditati e i Centri di Valutazione del Ministero dell'interno e del Ministero della difesa, ai sensi dell'articolo 1, comma 7, lettera b), del D.L. 105/2019.

La legislazione vigente prevede l'adozione anche di un DPCM per definire le procedure di notifica degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici (art. 1, comma 3, DL 105/2019).

-

Certificazione di sicurezza dei prodotti ICT

Il Governo ha trasmesso lo schema di decreto legislativo A.G. 388 che attua la delega prevista dall'articolo 18 della legge di delegazione europea 2019-2020 (legge 22 aprile 2021, n. 53) volta all'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) n. 2019/881 del 17 aprile 2019, relativo all'Agenzia dell'Unione europea per la cibersicurezza (European Union Agency for Network and Information Security — ENISA) e al quadro europeo della certificazione.

Più precisamente, il provvedimento dà attuazione ad alcune disposizioni del titolo III del regolamento, relative alla certificazione della cibersicurezza dei prodotti, dei servizi e dei processi relativi alle tecnologie dell'informazione e della comunicazione (ICT).

Si ricorda che i regolamenti dell'Unione europea sono atti giuridici definiti nell'articolo 288 del trattato sul funzionamento dell'Unione europea (TFUE). Sono di applicazione generale, vincolanti in tutti i loro elementi e direttamente applicabili in tutti i Paesi membri, senza dovere essere trasposti in una legge nazionale. Tuttavia, in alcuni casi - come in quello in esame - è lo stesso regolamento che rinvia alla adozione di norme nazionali per la sua piena applicabilità. In particolare, al fine di dare attuazione al regolamento sulla cibersicurezza - principalmente con riferimento agli articoli 58, 60, 61, 63, 64 e 65 dello stesso - è necessario che ciascuno Stato membro adotti alcuni interventi normativi a livello nazionale.

Dossier

Certificazione di sicurezza dei prodotti ICT in attuazione del regolamento UE sulla cibersicurezza
https://temi.camera.it/dossier/OCD18-16758/certificazione-sicurezza-prodotti-ict-attuazione-del-regolamento-ue-sulla-cibersicurezza.html

---

La Strategia nazionale di Cybersicurezza

Il 18 maggio 2022 il Comitato Interministeriale per la Cybersicurezza, presieduto dal Presidente del Consiglio dei ministri ha approvato la Strategia nazionale di cybersicurezza (2022-2026) e l'annesso Piano di implementazione.

Attraverso i due documenti, il Governo mira ad affrontare una pluralità di sfide quali: il rafforzamento della resilienza nella transizione digitale del sistema Paese; il conseguimento dell'autonomia strategica nella dimensione cibernetica; l'anticipazione dell'evoluzione della minaccia cyber; la gestione di crisi cibernetiche.