Marco Berruti - Fabio Gaggero

I pilastri normativi della sicurezza cibernetica*

SOMMARIO: 1. Introduzione - 2. La *Network and Information Security* (Direttiva NIS 2016/1148) e la sua attuazione nazionale - 3. Il *Cybersecurity Act* (Reg. 2019/881) tra ENISA e certificazioni - 4. La progettazione dell'architettura nazionale cibernetica: l'istituzione del Perimetro Nazionale di Sicurezza (d.l. 105/2019) - 5. L'intricata fase di costruzione del Perimetro (provvedimenti attuativi del d.l. 105/2019) - 6. Le varianti in corso d'opera: l'Agenzia per la Cybersicurezza Nazionale e la gestione del Perimetro (d.l. 82/2021) - 7. I prossimi appuntamenti normativi: una previsione (provvedimenti attuativi del d.l. 82/2021) - 8. Conclusioni

1. *Introduzione*

Il presente contributo si pone l'obiettivo di ricostruire in forma schematica l'articolato quadro normativo, nazionale ed europeo, su cui oggi si fonda la disciplina della sicurezza cibernetica dello Stato e delle sue infrastrutture.

Innanzitutto, pare opportuno segnalare come la varietà delle fonti abbia imposto una selezione degli argomenti da trattare. In particolare, si è scelto di escludere dall'analisi tutti quegli atti che, seppur contenenti disposizioni in materia di sicurezza dei sistemi informatici e delle reti, si occupano principalmente di tematiche differenti.

Ne deriva che lo schema che ci si appresta a presentare non dev'essere inteso come omnicomprensivo di tutti i possibili adempimenti gravanti sugli operatori interessati, in quanto alcuni di essi derivano da fonti che regolano precipuamente altri settori del diritto. Il riferimento è per esempio agli obblighi previsti dalla normativa "privacy"[1], che – attesa la stretta correlazione tra la sicurezza dei dati personali e la sicurezza delle infrastrutture ove essi sono conservati – include anche disposizioni attinenti al macro-tema della cybersecurity, o agli obblighi derivanti dall'adesione al framework eIDas[2].

Si deve poi registrare che durante la redazione dello schema è intervenuta la conversione in legge del d.l. n. 82/2021 recante, tra le altre cose, disposizioni in ordine all'istituzione dell'Agenzia per la cybersicurezza nazionale. Ciò ha reso necessario aggiornare in itinere la rassegna delle fonti, inserendo nella parte descrittiva di ogni capitolo (come pure nel prospetto conclusivo del contributo) un focus sulle principali novità e modifiche nel frattempo introdotte dal legislatore.

Fatte queste doverose premesse, la ricerca vuole costituire un'utile mappa per la lettura e lo studio del settore. Si è scelto pertanto di sviluppare l'analisi ricorrendo ad alcune semplificazioni grafiche.

La scansione del lavoro, infatti, passa attraverso l'individuazione e la descrizione delle diverse componenti architettoniche di un ipotetico "tempio" normativo, rappresentativo della composita disciplina su cui oggi si fonda la sicurezza cibernetica nazionale.

La similitudine pare efficace, soprattutto visto il carattere multilivello delle fonti. Segnatamente, alla base della struttura si collocano gli interventi dell'Unione europea, che costituiscono oggi il cuore della strategia eurounitaria in materia di cybersecurity. Su queste fondamenta, quindi, si erige la normativa nazionale, dipanandosi simbolicamente lungo le colonne portanti dell'edificio fino a raggiungerne la sommità.

---

* Il presente elaborato è destinato agli atti del convegno *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, Genova, 18-19 giugno 2021 (in corso di pubblicazione). Esso è il frutto delle riflessioni congiunte degli autori: tuttavia, vanno attribuiti a Fabio Gaggero i paragrafi 1-4 e a Marco Berruti i paragrafi 5-8.

[1] Basti pensare alle norme relative al processo di notificazione del cd. *data breach* (art. 33 GDPR) e all'obbligo di adozione di misure adeguate al rischio (art. 32 GDPR).

[2] Il riferimento è al regolamento (UE) 2014/910 in materia di identificazione elettronica.

Decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133 – Modalità e procedure per l'istituzione e il funzionamento del perimetro di sicurezza nazionale

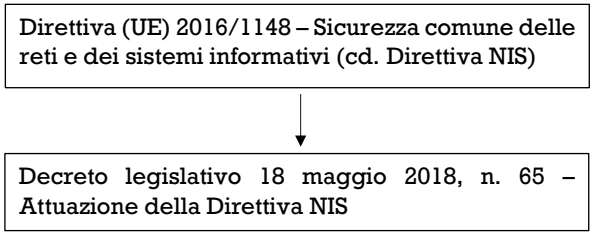
Provvedimenti attuativi del Decreto-legge 21 settembre 2019, n. 105

Regolamento (UE) 2019/881 – Riorganizzazione dell'ENISA e istituzione del Quadro europeo di certificazione volontaria della cibersicurezza (cd. Cybersecurity Act)

Direttiva (UE) 2016/1148 – Sicurezza comune delle reti e dei sistemi informativi (cd. Direttiva NIS)

Decreto legislativo 18 maggio 2018, n. 65 – Attuazione della Direttiva NIS

Decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla Legge 4 agosto 2021, n. 109 – Definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale



2. *La Network and Information Security (Direttiva NIS 2016/1148) e la sua attuazione nazionale*

Partendo dalle fondamenta del "tempio", la prima fonte che si incontra è la direttiva (UE) 2016/1148, la cosiddetta "Direttiva NIS", recepita dal nostro ordinamento con il decreto legislativo n. 65 del 2018.

Essa rappresenta un primo tentativo di armonizzazione dei livelli di sicurezza delle reti e dei sistemi informativi, obiettivo che viene perseguito attraverso l'introduzione di definizioni comuni e la predisposizione di un sistema di coordinamento integrato a livello dell'Unione, il quale prevede la designazione delle autorità nazionali NIS e del punto di contatto unico nazionale, nonché la creazione dei gruppi d'intervento per la sicurezza informatica in caso di incidente (CSIRT).

Le autorità nazionali hanno il compito di individuare gli operatori di servizi essenziali (OSE) e di garantire la corretta l'applicazione della normativa, attraverso l'esercizio di potestà ispettive e sanzionatorie.

Recentemente, dopo diversi rimandi alla necessità di un'unica autorità competente, si è finalmente giunti alla creazione di un'Agenzia per la cybersicurezza nazionale (da qui in avanti solo ACN o Agenzia). Il decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni dalla legge 4 agosto 2021, n. 109, ha quindi modificato il precedente sistema che vedeva una molteplicità di autorità nazionali suddivise per settore. A queste si affianca ora l'ACN, la quale lascia invariate le loro prerogative settoriali, riguardanti l'individuazione concreta degli OSE, ma accentra a sé le potestà ispettive e di controllo, come si evince dalle modifiche agli artt. 7 e 19 del d.lgs. n. 65 del 2018, e dall'art. 7 del d.l. 82 del 2021.

In aggiunta, proprio per garantire il coordinamento e la collaborazione delle diverse autorità settoriali con la nuova ACN, è stato creato presso quest'ultima un apposito comitato tecnico di raccordo, la cui organizzazione sarà definita con decreto del Presidente del Consiglio dei ministri. Di conseguenza, anche la tenuta del registro contenente l'elenco nazionale degli OSE viene trasferita dal Ministero dello Sviluppo Economico all'ACN. Del suo aggiornamento si occuperà ogni due anni l'Agenzia, previa proposta delle singole autorità settoriali.

L'ACN costituisce anche il nuovo punto di contatto unico NIS, ex art. 7 del d.l. 82 del 2021, funzione che prima era ricoperta dal Dipartimento delle informazioni per la sicurezza (DIS), istituito presso la Presidenza del Consiglio dei ministri. Tutte le funzioni di coordinamento con le autorità NIS degli altri stati membri, con il gruppo di cooperazione, nonché con l'autorità Garante per la protezione dei dati personali, verranno pertanto svolte dall'ACN. Parimenti, tutti i rinvii al DIS ancora presenti nel decreto, relativi alla procedura di notificazione degli incidenti, devono intendersi riferiti all'ACN.

Con il venir meno del ruolo di punto di contatto unico del DIS, emerge anche la necessità di una nuova collocazione per il CSIRT, le cui strutture e competenze ora vengono accorpate nell'ACN, sotto la nuova denominazione di "CSIRT Italia", ex art dall'art. 7, c. 3, del d.l. 82 del 2021.

Pressoché invariate, invece, rimangono le competenze della Presidenza del Consiglio dei ministri, alla quale spetta in via esclusiva il compito di adottare la strategia nazionale di cybersicurezza, la cui predisposizione però è affidata all'ACN, in base all'art. 7, c. 1, lett. b) del d.l. 82 del 2021.

Per quanto riguarda l'adozione di tale strategia, oltre a una mera differenza terminologica (il termine "sicurezza cibernetica" è infatti stato sostituito con il termine "cybersicurezza"), appare altresì rilevante la previsione secondo cui il piano non debba più essere comunicato direttamente dalla Presidenza del Consiglio alla Commissione europea, in quanto alla sua trasmissione provvederà direttamente l'ACN, con una notevole semplificazione nei rapporti.

Per concludere, la restante normativa del "framework NIS" si occupa degli obblighi in materia di sicurezza e notifica degli incidenti a carico degli operatori di servizi essenziali (OSE) e dei fornitori di servizi digitali (FSD). Anche se rispetto a tale settore non si registrano interventi modificativi da parte del d.l. 82/2021, va comunque ribadito che i relativi controlli non sono più svolti dalle singole autorità settoriali, ma dall'ACN, la quale acquisisce anche il ruolo di destinatario ultimo delle notificazioni delle violazioni della cybersicurezza provenienti dal CSIRT.

Network NIS

Obiettivi

1. Migliorare la capacità degli Stati membri nella gestione della sicurezza delle reti e dei sistemi di informazione e nella risposta agli incidenti.
2. Promuovere una cultura di gestione del rischio tra gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (FSD).
3. Implementare la cooperazione sia tecnica sia strategica a livello di Unione.

Oggetto

Ogni Stato membro deve:

I. identificare gli operatori dei servizi essenziali (OSE);
II. designare una o più autorità (cd. autorità NIS) preposte alla vigilanza degli OSE e dei FDS;
III. individuare un punto di contatto unico incaricato di coordinare le autorità di cui al p. II e di attuare la cooperazione transfrontaliera;
IV. istituire un gruppo di intervento per la sicurezza informatica in caso di incidente (Computer Emergency Response Team - CSIRT), chiamato a trattare gli incidenti;
V. adottare una strategia nazionale per la sicurezza della rete e dei sistemi informativi;
VI. definire gli obblighi in capo agli OSE ed ai FDS in materia di sicurezza e notifica degli incidenti.

Definizioni

1. Reti e sistemi di informazione: a) reti di comunicazione elettronica;
   (art. 4, n. 1) b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati tra loro, uno o più dei quali trattano in modo automatico dati digitali;
   c) i dati digitali conservati, trattati, estratti o trasmessi per mezzo delle reti o dei dispositivi di cui alle lett. a) e b).
2. Sicurezza delle e dei sistemi di informazione: la capacità di una rete o di un sistema di
   (Art. 4, n. 2) resistere a ogni azione che comprometta:
   I) la disponibilità,
   II) l'autenticità,
   III) l'integrità o
   IV) la riservatezza dei dati conservati, trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistema informativo.
3. Incidente: ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi. (art. 4, n. 7)
4. Rischio: ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi di informazione. (art. 4, n. 9)
5. Operatori di servizi essenziali (OSE): qualsiasi soggetto pubblico o privato che, all'interno del settore bancario, sanitario, dell'energia, dei trasporti, delle infrastrutture dei mercati finanziari, delle infrastrutture digitali o della fornitura e distribuzione di acqua potabile, con sede nel territorio nazionale fornisce:
   I. un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
   II. un servizio la cui fornitura dipenda da almeno una rete o un sistema informativo;
   III. un servizio su cui un incidente avrebbe effetti negativi rilevanti. (art. 5, § 2)
6. Fornitori di servizi digitali (FSD): qualsiasi persona giuridica che, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale, fornisca un servizio digitale del seguente tipo: e-commerce, motori di ricerca, cloud computing. (art 4, n. 6)

Autorità NIS

Autorità competente	Ambito di competenza
Ministero dello Sviluppo Economico (MISE)	→Settore dell'energia →Settore delle infrastrutture digitali
Ministero delle Infrastrutture	→Settore dei trasporti
Ministero dell'Economia e delle Finanze, Banca d'Italia e Consob	→ Settore bancario → Settore delle infrastrutture dei mercati finanziari
Ministero della Salute, Regioni e Province Autonome	→ Settore sanitario
Ministero della Transizione ecologica, Regioni e Province Autonome	→Settore della fornitura e distribuzione dell'acqua potabile

Cura la tenuta dell'elenco nazionale degli OSE

1. Identificano per ciascun settore gli OSE con sede nel territorio nazionale, stilando un apposito elenco da aggiornare almeno ogni due anni.

2. Predispongono le linee guida per la notifica degli incidenti.

3. Sono responsabili dell'attuazione del decreto e vigilano sulla sua applicazione.

4. Partecipano ai programmi di cooperazione europea al fine di elaborare ed adottare orientamenti sulle circostanze in cui gli OSE sono tenuti a notificare gli incidenti.

5. Esercitano poteri di ispezione e verifica per valutare l'adeguatezza delle misure tecniche e organizzative adottate dagli OSE per la gestione dei rischi relativi alla sicurezza delle loro reti e sistemi informativi.

6. Accertano le violazioni commesse dagli OSE e dagli FSD in materia di sicurezza e notifica degli incidenti e irroga le relative sanzioni amministrative.

Criteri per l'identificazione OSE:

- il soggetto fornisce un servizio essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
- la fornitura del servizio dipende dalla rete e dai sistemi informativi;
- un incidente avrebbe effetti negativi rilevanti sulla fornitura del servizio medesimo, tenuto conto dei seguenti parametri:
  a) il numero di utenti che dipendono dal servizio fornito;
  b) la dipendenza di altri settori strategici dal servizio fornito;
  c) l'impatto che gli incidenti potrebbero avere, in termini di entità e durata, sulle attività economiche e sociali o sulla pubblica sicurezza;
  d) la quota di mercato dell'operatore del servizio;
  e) la diffusione geografica relativamente all'area che potrebbe essere interessata da un incidente;
  f) l'importanza dell'operatore per il mantenimento di un livello sufficiente del servizio, tenendo conto della disponibilità di strumenti alternativi per la fornitura di tale servizio.

CSIRT

Dipartimento delle Informazioni per la Sicurezza (**DIS**)

Presidenza del Consiglio dei Ministri

Sistema di informazione per la sicurezza della Repubblica

La sua organizzazione e il suo funzionamento sono disciplinati dal d.P.C.M. 8 agosto 2019.

Riceve le notifiche relative a incidenti da parte degli OSE e dei FSD.

Informa le autorità competenti NIS e il Punto di contatto in merito alle notifiche di incidenti trasmesse.

Sulla base delle informazioni fornite in sede di notifica, informa gli altri Stati membri in cui l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali.

Dirama preallarmi, allerte e annunci in merito ai rischi e agli incidenti.

Preserva la sicurezza e gli interessi commerciali dei notificanti, nonché la riservatezza delle informazioni fornite nella notifica.

Ove le circostanze lo consentano, fornisce al notificante le informazioni relative al seguito della notifica stessa, nonché le informazioni che possono facilitare un trattamento efficace dell'incidente.

Inoltra tempestivamente le notifiche al Dipartimento informazioni per la sicurezza incaricato della gestione dell'incidente, ai sensi delle direttive del Presidente del Consiglio dei Ministeri e del CISR.

Previa valutazione di tale Dipartimento, l'autorità NIS, d'intesa con il CSIRT, informa il pubblico riguardo al singolo incidente.

Partecipa alla **rete di CSIRT**, composta da rappresentanti dei CSIRT degli Stati membri e del CERT-UE.

È designato quale **Punto di contatto unico**

- Svolge una funzione di collegamento tra le autorità NIS nazionali.
- Garantisce la cooperazione transfrontaliera delle autorità NIS con le autorità competenti degli altri Stati membri.
- Partecipa alle attività del gruppo di cooperazione europeo, condividendo e scambiando buone pratiche, esperienze e informazioni.
- Trasmette annualmente al gruppo di cooperazione europeo una relazione sulle notifiche ricevute.
- Consulta l'organo del Ministero dell'Interno per la sicurezza e la regolarità dei servizi di telecomunicazione ed il Garante Privacy e con essi collabora.
- Su richiesta dell'autorità competente NIS o del CSIRT, trasmette le notifiche di incidente ai punti di contatto unici degli altri Stati membri.

Adotta la Strategia nazionale di sicurezza cibernetica, sentito il Comitato interministeriale per la Sicurezza della Repubblica (CISR).

Operatori di Servizi Essenziali (OSE)

Fornitori di Servizi Digitali (FSD)

Sono escluse le imprese che hanno meno di 50 dipendenti e un fatturato o bilancio annuo non superiore ai 10 milioni di Euro (cioè le piccole e le microimprese).

Adottano:

I. misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano per la fornitura dei loro servizi;

II. misure per prevenire e minimizzare l'impatto di incidenti a carico della rete e dei sistemi informativi, al fine di assicurare la continuità dei loro servizi.

Per l'adozione di tali misure e per l'individuazione del rischio esistente, i FSD tengono conto dei seguenti elementi:

- sicurezza dei sistemi e degli impianti;
- trattamento degli incidenti;
- gestione della continuità operativa;
- monitoraggio, audit e test;
- conformità con le norme internazionali

Gli OSE devono altresì fornire la prova dell'effettiva attuazione delle politiche di sicurezza svolto dall'autorità competente NIS o da un revisore abilitato e, in quest'ultimo caso, metterne a disposizione dell'autorità competente NIS i risultati, inclusi gli elementi di prova.

Forniscono alla competente autorità NIS le informazioni necessarie per valutare la sicurezza della loro rete e dei loro sistemi informativi, compresi i documenti relativi alle politiche di sicurezza.

I soggetti diversi dagli OSE e dai FSD possono notificare, su base volontaria, gli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati.

Notificano al CSIRT e, per conoscenza, all'autorità competente NIS, senza giustificato ritardo, gli incidenti aventi un impatto rilevante sulla continuità e sulla fornitura del servizio.

Quanto agli OSE…

a) il numero di utenti interessati dalla perturbazione del servizio essenziale;
b) la durata dell'incidente;
c) la diffusione geografica relativamente all'area interessata dall'incidente.

Al fine di determinare la rilevanza dell'impatto di un incidente, sono presi in considerazione i seguenti parametri:

Quanto ai FSD…

a) il numero di utenti interessati dall'incidente, in particolare gli utenti che dipendono dal servizio digitale per la fornitura dei propri servizi;
b) la durata dell'incidente;
c) la diffusione geografica relativamente all'area interessata dall'incidente;
d) la portata della perturbazione del funzionamento del servizio;
e) la portata dell'impatto sulle attività economiche e sociali.

Le notifiche includono le informazioni che consentono al CSIRT di determinare la rilevanza di un eventuale impatto transfrontaliero. La notifica non espone la parte che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente.

Regolamento (UE) 2019/881 – Riorganizzazione dell'ENISA e istituzione del Quadro europeo di certificazione volontaria della cibersicurezza (cd. Cybersecurity Act)

3. *Il Cybersecurity Act (Reg. 2019/881) tra ENISA e certificazioni*

La seconda fonte su cui si regge l'intera "architettura" normativa è costituita dal regolamento (UE) 2019/881, il cosiddetto "Cybersecurity Act", che abroga il precedente regolamento (UE) 2013/526 e, al contempo, assegna all'ENISA (l'Agenzia dell'Unione europea per la cybersicurezza) la missione "permanente" di curare, vigilare, coordinare e migliorare la sicurezza cibernetica tra gli Stati membri. L'agenzia aveva iniziato i suoi lavori il 14 marzo 2004 in forza del regolamento (CE) 2004/460, che le conferiva un mandato di soli nove anni e sei mesi. Il successivo regolamento (UE) 2013/526 aveva rinnovato il mandato fino al 2020. La novità però non consiste semplicemente nella stabilizzazione delle funzioni dell'agenzia, ma nell'introduzione di un quadro europeo per la certificazione della cybersicurezza, i cui effetti hanno iniziato a decorrere dal 21 giugno 2021. Lo scopo è quello di favorire il mercato europeo e la circolazione dei servizi informatici, attraverso l'armonizzazione degli standard di sicurezza nazionali.

La presenza di una certificazione, in effetti, garantisce la predisposizione di misure di sicurezza adeguate al livello di rischio, in coerenza con diversi livelli di affidabilità per il prodotto o per il servizio ("di base", "sostanziale" o "elevato").

Il sistema di certificazioni, poi, pone le condizioni per una concorrenza fondata sulla migliore qualità della sicurezza informatica, che viene resa intellegibile agli utenti, dal momento che i consumatori possono semplicemente fare riferimento alle certificazioni senza doversi preoccupare di svolgere un puntuale (e costoso) controllo dell'affidabilità del prodotto o del servizio.

Infine, si segnala che, ai sensi dell'art. 7, c. 1, lett. e) del d.l. 82 del 2021, la nuova ANC assumerà anche la funzione di autorità nazionale di certificazione, la cui istituzione è espressamente prevista dal "Cybersecurity Act", acquisendo tutte le funzioni dapprima svolte dal Ministero dello sviluppo economico.

Cybersecurity Act

Obiettivi

Garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza all'interno dell'Unione, allo scopo di proteggere dalle minacce informatiche le reti e i servizi informativi.

Oggetto

I. Definizione degli obblighi, dei compiti e degli aspetti organizzativi relativi all'ENISA (Agenzia dell'Unione europea per la cibersicurezza);
II. Predisposizione di un sistema europeo di certificazione volontaria della cibersicurezza dei prodotti, servizi e processi delle tecnologie dell'informazione e delle comunicazioni (TIC).

Definizioni

1. Cibersicurezza: l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche. (art. 2, n. 1)
2. Minaccia informatica: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti e altre persone. (art. 2, n. 8)
3. Sistema europeo di certificazione della cibersicurezza: una serie completa, di regole, requisiti tecnici, norme e procedure stabiliti a livello di Unione e che si applicano alla certificazione o alla valutazione della conformità di specifici prodotti, servizi e processi TIC. (art. 2, n. 9)

ENISA – The European Union Agency for Cybersecurity

Mandato e obiettivi

1. Conseguire un elevato livello comune di cibersicurezza in tutta l'UE, sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi nel miglioramento della cibersicurezza.
2. Fungere da punto di riferimento per pareri e competenze in materia di cibersicurezza per i soggetti di cui al punto 1 nonché per altri portatori di interessi pubblici o privati.
3. Ridurre le frammentazioni nel mercato interno, promuovendo l'uso della certificazione europea della cibersicurezza.
4. Incentivare un elevato livello di consapevolezza, promuovendo la cd. "igiene e alfabetizzazione informatica", tra i cittadini, le organizzazioni e le imprese.

Compiti

1. Sviluppo e attuazione delle politiche e della normativa dell'Unione, attraverso pareri, orientamenti e buone prassi
2. Sviluppo delle capacità di prevenzione, rilevazione, reazione e analisi delle minacce e degli incidenti informatici
3. Cooperazione operativa tra Stati membri, istituti, organi e organismi UE, compresa la CERT-UE, e i portatori di interessi
4. Sviluppo e attuazione della politica UE in materia di certificazione della cibersicurezza dei prodotti, servizi e processi ICT
5. Analisi delle tecnologie emergenti e del loro impatto sulla cibersicurezza
6. Sensibilizzazione dell'opinione pubblica sui rischi connessi alle minacce informatiche
7. Ricerca e innovazione
8. Cooperazione con paesi terzi e organizzazioni internazionali

Organizzazione

- *Consiglio di amministrazione*, composto da un rappresentante per Stato membro oltre che da due rappresentanti della Commissione:
  → stabilisce gli orientamenti generali delle attività dell'agenzia;
  → assicura che l'agenzia serva al meglio il mandato conferitole dal regolamento.
- *Comitato esecutivo*, composto da cinque membri scelti tra i componenti del cda:
  → prepara le decisioni che dovrà assumere il cda.
- *Direttore esecutivo*, indipendente, nominato dal cda:
  → attua le decisioni del cda;
  → risponde al cda e riferisce al Parlamento europeo e al Consiglio.
- *Gruppo consultivo ENISA*, composto da esperti riconosciuti:
  → rappresenta i portatori di interessi;
  → consiglia l'ENISA ai fini dello svolgimento dei suoi compiti
- *Gruppo dei portatori di interessi per la certificazione della cibersicurezza*, composto da esperti riconosciuti:
  → rappresenta le istanze dei portatori d'interessi per la certificazione della cibersicurezza.
- *Rete dei funzionari nazionali di collegamento*, composta da rappresentanti di tutti gli Stati membri:
  → agevola lo scambio di informazioni tra ENISA e i paesi dell'UE;
  → sostiene l'ENISA nell'attività di diffusione delle sue raccomandazioni.

Quadro europeo di certificazione della cibersicurezza

Obiettivi

Migliorare le condizioni di funzionamento del mercato interno:

1. aumentando il livello di cibersicurezza all'interno dell'UE;
2. rendendo possibile un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza, allo scopo di creare un mercato unico digitale per i prodotti, servizi e processi ICT.

La certificazione di cibersicurezza è volontaria, salvo quanto diversamente specificato dal diritto dell'Unione o dagli Stati membri (art. 56).

Tappe del processo di elaborazione di un sistema di certificazione

I. La Commissione europea chiede all'ENISA la formulazione di una proposta di sistema o la revisione di un sistema europeo già esistente.
II. Previa consultazione dei portatori d'interesse, l'ENISA prepara una proposta che soddisfi i livelli di sicurezza, di affidabilità e gli altri requisiti indicati dal regolamento (artt. 51, 52 e 54).
III. La Commissione adotta gli atti necessari a dare esecuzione alla proposta.
IV. Almeno ogni cinque anni l'ENISA valuta il sistema di certificazione europeo adottato dalla Commissione, tenendo conto del riscontro ricevuto dalle parti interessate.

Il sistema di certificazione deve:

a) specificare il livello di affidabilità del prodotto, servizio o processo ICT (livello "di base", "sostanziale" o "elevato");
b) permettere ai fabbricanti e ai fornitori del prodotto, servizi o processo ICT con basso rischio al livello di affidabilità di base di produrre un'autovalutazione della conformità;
c) indicare l'oggetto e l'ambito di applicazione del sistema di certificazione, compresi il tipo e le categorie dei prodotti, servizi e processi ICT coperti (e gli altri elementi di cui all'art. 54).

Soggetti

• *Autorità nazionali di certificazione della cibersicurezza*, designata da ciascun Stato membro:
→ vigilano sulla corretta applicazione (all'interno dei confini nazionali) delle regole fissate in uno o più sistemi europei di certificazione;
→ autorizzano gli organismi di valutazione della conformità;
→ esercitano poteri istruttori, ispettivi e sanzionatori nei confronti degli organismi di valutazione della conformità dei fabbricanti e fornitori di prodotti, servizi e processi ICT;
→ trattano i reclami delle persone fisiche o giuridiche in ordine al rilascio dei certificati europei di cibersicurezza;
→ rilasciano certificati europei di cibersicurezza riferiti ad un livello di affidabilità "elevato" del prodotto, servizio o processo ICT

• *Organismi di valutazione della conformità*, enti terzi, indipendenti dall'organizzazione o dai prodotti, servizi o processi che valuta, dotati di solide competenze tecniche professionali:
→ rilasciano certificati europei di cibersicurezza riferiti ad un livello di affidabilità "di base" o "sostanziale" del prodotto, servizio o processo ICT.

• *Gruppo europeo per la certificazione della cibersicurezza (ECCG)*, composto dai rappresentanti delle autorità nazionali di certificazione della cibersicurezza:
→ coadiuva e consiglia la Commissione europea e l'ENISA nel processo di elaborazione e revisione dei sistemi europei di certificazione.

Decreto-legge 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133 – Modalità e procedure per l'istituzione e il funzionamento del perimetro di sicurezza nazionale

4. *La progettazione dell'architettura nazionale cibernetica: l'istituzione del Perimetro Nazionale di Sicurezza (d.l. 105/2019)*

Seguendo la metafora del tempio, alla sua sommità "si staglia" il decreto-legge 21 settembre 2019, n. 105, poi convertito con modificazioni dalla legge 18 novembre 2019, n. 133, che istituisce il Perimetro di sicurezza nazionale. Si tratta di un sistema complesso di obblighi di sicurezza, controlli e notifiche, che ha il fine ultimo di assicurare un elevato livello di sicurezza di tutte quelle reti e di tutti quei servizi dai quali dipende l'esercizio di funzioni e/o di interessi essenziali dello Stato.

La logica di fondo è quella di estendere anche all'ambito "cyber" i poteri speciali che l'Esecutivo può esercitare sugli assetti societari delle imprese operanti nei settori della difesa e della sicurezza nazionale, nonché in altri settori considerati strategici, azionando il cosiddetto "*Golden power*".

Per raggiungere questo obiettivo, il decreto in esame interviene direttamente sul decreto legislativo 15 marzo 2012, n. 21, introducendo la facoltà per il Governo di esercitare i "poteri speciali" anche nei confronti di contratti e accordi necessari per la fornitura di servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.

Tale riforma non è altro che una delle modalità di realizzazione dell'obiettivo principale a cui tende il d.l. 105/2019, vale a dire prendere definitivamente atto della crescente digitalizzazione delle attività svolte nell'ambito dei settori strategici e, pertanto, implementare i controlli sulla sicurezza degli approvvigionamenti, che ormai sono costituiti in gran parte da forniture di componenti hardware o software.

Ciò premesso, similmente a quanto avviene nell'ambito della normativa NIS in merito all'individuazione degli OSE e dei FSD, anche il funzionamento del Perimetro di sicurezza cibernetica passa attraverso la definizione dei soggetti sottoposti agli obblighi di notificazione delle operazioni di acquisizione, nonché degli incidenti aventi un impatto sui loro sistemi. Questi attori sono vincolati a tenere un elenco aggiornato delle reti, dei sistemi informativi e dei propri servizi informatici, da trasmettere all'ACN, che nel frattempo ha acquisito le competenze assegnate in origine alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico.

Decreto-legge 105/2019

Obiettivi

Assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, che esercitano una funzione essenziale dello Stato o hanno carattere strategico per gli interessi del Paese e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale.

Oggetto

I. Modalità, procedure e termini per l'istituzione del Perimetro di sicurezza nazionale cibernetica (art. 1).
II. Misure di raccordo tra il Perimetro di sicurezza cibernetica e la normativa in materia di esercizio dei poteri speciali sui servizi di comunicazione elettronica a banda larga con tecnologia 5G (art. 3).
III. Modifiche alla disciplina dei poteri speciali, in un'ottica di coordinamento con la normativa eurounitaria sul controllo degli investimenti esteri diretti (art. 4 bis).

Definizioni

1. Poteri speciali (*Golden Power*): poteri di intervento riconosciuti in capo al Governo, il quale – ai sensi del decreto-legge 15 marzo 2012, n. 21 – li esercita al fine di salvaguardare gli assetti delle imprese operanti in ambiti ritenuti strategici e di interesse nazionale (settore: Difesa e Sicurezza nazionale, Tecnologia 5G, Energia, Trasporti e Comunicazioni), in presenza di operazioni societarie che rappresentano una minaccia di grave pregiudizio per gli interessi pubblici. Nel rispetto del principio di proporzionalità e ragionevolezza, sono esercitabili i seguenti poteri:
   a) opposizione all'acquisto di partecipazioni;
   b) veto all'adozione di delibere societarie;
   c) imposizione di specifiche prescrizioni e condizioni.
2. Investimento estero diretto: un investimento di qualsiasi tipo effettuato da una persona fisica o giuridica di un paese extra-UE, volto a stabilire o mantenere un legame durevole e diretto con un'impresa, al fine di esercitare un'attività economica in uno Stato membro (art. 2, n. 1 e 2, reg. 2019/452).

Funzionamento del Perimetro di sicurezza nazionale cibernetica

Predispongono e aggiornano un elenco delle reti, dei sistemi informativi e dei servizi informatici di loro pertinenza, dal cui malfunzionamento, interruzione ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale. L'elenco è trasmesso a:

Soggetti pubblici

Soggetti privati

- Hanno una sede nel territorio nazionale.
- Esercitano una funzione o un servizio essenziale per lo Stato.
- Possono corrispondere agli OSE e ai FSD di cui al d.lgs. 65/2018.

La comunicazione comprende anche una valutazione del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego

Se intendono procedere, anche per il tramite di centrali di committenza, all'affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle loro reti e sistemi informativi ne danno comunicazione al:

Notificano gli incidenti aventi impatto sulle reti, sistemi e servizi ICT iscritte nell'apposito elenco al:

CSIRT

DIS

Direzione generale per lo sviluppo della prevenzione e tutela informatiche - Ministero dell'Interno

Centro di valutazione e certificazione nazionale – CVCN

istituito presso il

Il Presidente del Consiglio, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi informativi, può disporre, su deliberazione del CISR, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o più apparati o prodotti ICT.

per i soggetti pubblici

Presidenza del Consiglio dei Ministri

Ministero dello Sviluppo Economico

per i soggetti privati

Entro 45 giorni, avvia delle verifiche, all'esito delle quali:

Impone test di software e hardware e/o condizioni

Non si pronuncia

La procedura di affidamento prosegue

Esercitano poteri di verifica, ispezione e sanzione nell'ambito degli approvvigionamenti ICT

I bandi di gara e i contratti sono integrati con clausole che condizionano, sospensivamente o risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test (da concludere entro 60 giorni).

- Definisce metodologie di verifica e test.
- Si avvale di laboratori accreditati.
- Adotta schemi di certificazione cibernetica.

Le <u>linee programmatiche</u> del d.l. 105/2019 per l'istituzione del Perimetro nazionale di sicurezza cibernetica

• Definire le modalità e i criteri procedurali di individuazione delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati inclusi nel Perimetro di sicurezza nazionale cibernetica (art. 1, comma 2, lett a). • Determinare i criteri con i quali i soggetti inclusi nel Perimetro predispongono e aggiornano gli elenchi delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza (art. 1, comma 2, lett b).	✓ Criteri individuati dal d.P.C.M. 30 luglio 2020, n. 131
Stilare l'elenco dei soggetti inclusi nel Perimetro, comunicando agli interessati l'avvenuta iscrizione nell'elenco medesimo (art. 1, comma 2 bis).	✓ Lista approvata il 25 novembre 2020 (con atto amministrativo del Presidente del Consiglio dei Ministri non soggetto a pubblicazione) e aggiornata il 15 giugno 2021
• Specificare le procedure in base alle quali i soggetti inclusi nel Perimetro notificano al CSIRT gli incidenti aventi impatto sulle reti, sui sistemi informativi e sui servizi informatici di loro pertinenza (art. 1, comma 3, lett. a). • Stabilire le misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici dei soggetti coinvolti nel Perimetro, tenendo conto degli standard definiti a livello internazionale ed eurounitario (art. 1, comma 3, lett. b).	✓ Procedure definite dal d.P.C.M. 14 aprile 2021, n. 81
Disciplinare le procedure, le modalità e i termini con cui: • i soggetti inclusi nel Perimetro comunicano al Centro di valutazione e certificazione (CVCN) l'intenzione di procedere all'affidamento di beni, sistemi e servizi ICT destinati ad essere impiegati per l'espletamento delle loro funzioni (art. 1, comma 6, lett. a); • i soggetti fornitori di beni, sistemi e servizi ICT collaborano alle attività di verifica e test sulla sicurezza della loro fornitura (art. 1, comma 6, lett. b); • la Presidenza del Consiglio dei Ministri e il MISE svolgono i rispettivi poteri ispettivi e di verifica (art. 1, comma 6, lett. c).	→ d.P.R. 5 febbraio 2021, n. 54 → d.P.C.M. per l'individuazione delle categorie di beni, servizi e sistemi ICT oggetto di valutazione del CVCN (d.P.C.M. 15 giugno 2021) → d.P.C.M. per la definizione dei criteri di accreditamento dei laboratori di cui il CVCN può avvalersi per l'esercizio delle sue funzioni (in attesa di definizione)

5. *L'intricata fase di costruzione del Perimetro (provvedimenti attuativi del d.l. 105/2019)*

La delicatezza e, al tempo stesso, l'ambiziosità degli obiettivi perseguiti dal decreto-legge 105/2019 hanno reso particolarmente articolata la fase di attuazione del Perimetro, sviluppatasi attraverso l'emanazione di una lunga serie di d.P.C.M. e regolamenti governativi, simbolicamente rappresentati dalle colonne del "tempio"[3].

Il primo provvedimento attuativo risulta essere il d.P.C.M. 30 luglio 2020, n. 131, che (ex art. 1, c. 2, d.l. n. 105 del 2019) doveva essere approvato entro quattro mesi dall'entrata in vigore della legge di conversione del decreto (termine non rispettato a causa dell'esplosione della pandemia da Covid-19).

Tale provvedimento ha precisato i confini del Perimetro, fissando i criteri per l'individuazione dei soggetti pubblici e privati da includere nel Perimetro medesimo. Sulla base di tali criteri, il Presidente del Consiglio dei ministri ha quindi adottato il d.P.C.M. il 25 novembre 2020 mediante il quale ha stilato l'elenco degli operatori soggetti alle regole del Perimetro. Un primo aggiornamento di tale elencazione è avvenuto il 15 giugno 2021.

Il secondo tassello, invece, riguarda sia le modalità di notificazione degli incidenti da parte degli operatori inclusi nel Perimetro al CSIRT, sia le elevate misure di sicurezza che questi sono tenuti ad adottare e rispettare.

Tutto ciò ha ricevuto una concretizzazione normativa solo l'11 giugno 2021, a seguito della pubblicazione in Gazzetta Ufficiale del d.P.C.M. 14 aprile 2021, n. 81, malgrado, ai sensi art. 1, c. 3, del d.l. n. 105 del 2019, il decreto attuativo dovesse essere approvato entro dieci mesi dall'entrata in vigore della legge di conversione del decreto-legge.

Al momento, i soggetti coinvolti procedono alla notificazione degli incidenti solo in via sperimentale: l'obbligatorietà è fissata a partire dal 2022. Le formalità di notifica variano a seconda della gravità dell'incidente. Nel caso in cui il soggetto obbligato sia anche un OSE, un FSD oppure un operatore di comunicazioni elettroniche sottoposto alla disciplina e-privacy, la notifica assolve anche gli adempimenti della normativa "privacy" o della normativa "NIS", evitando così inutili duplicazioni.

Riguardo alle novità introdotte dal d.l. 82/2021, occorre qui registrare che la creazione dell'ACN influirà sulle formalità e sui rapporti con il CSIRT, che, a norma dell'art. 5 del d.P.C.M. in esame, è tenuto a trasmettere ogni notificazione al DIS, il quale a sua volta la ritrasmette ad un'altra serie di organi, tra i quali il Ministero dello sviluppo economico (per le notifiche provenienti da privati) e la Presidenza del Consiglio dei ministri (per le notifiche provenienti da enti pubblici).

Anche se la tale previsione non ha subìto alcuna modifica diretta da parte del d.l. 82 del 2021, il d.P.C.M. 81/2021 va interpretato in coerenza con quanto disposto con l'art. 7 del d.l. 82/2021 che dispone l'acquisizione da parte dell'ACN di tutte le funzioni del DIS, del Ministero dello sviluppo economico e della Presidenza del Consiglio dei ministri. A fortiori, anche tutti i rinvii a tali organi effettuati dal d.l. 105 del 2019 vanno oggi riferiti all'ACN.

[3] Nel momento in cui si scrive, l'attuazione del Perimetro non risulta ancora ultimata. Si stima che il perfezionamento del sistema introdotto dal d.l. 105/2019 si perfezioni entro la fine dell'autunno 2021.

La terza “colonna portante” del “tempio” è rappresentata dal d.P.R. 5 febbraio 2021, n. 54, che disciplina i meccanismi di controllo delle forniture di servizi e strumenti digitali, e che, secondo l’art. 1, c. 6, del d.l. n. 105 del 2019, doveva essere adottato entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto medesimo.

In primo luogo, il Regolamento detta le procedure, le modalità e i termini da seguire ai fini delle valutazioni effettuate dal centro di valutazione e certificazione nazionale (CVCN) e dai centri di valutazione (CV). Si rammenta che il CVCN, dapprima istituito presso il Ministero dello sviluppo economico, confluirà nella struttura dell’ACN, ex art. 7, c. 4, del d.l. 82 del 2021. Quest’ultimo, tra le altre cose, ha subordinato l’operatività del CVNC e dei CV all’adozione di un apposito d.P.C.M. sentita previamente l’Agenzia medesima.

In secondo luogo, il Regolamento indica i criteri per individuare le categorie di beni, servizi e sistemi ICT da sottoporre a valutazione. Nello specifico, esattamente com’è avvenuto per i soggetti da includere nel Perimetro, l’elenco completo è stato oggetto di un provvedimento ad hoc: il d.P.C.M. 15 giugno 2021.

Infine, il provvedimento in commento si preoccupa di descrivere le procedure, le modalità e i termini con cui le autorità competenti effettuano le attività di verifica e di ispezione. Nonostante l’art. 15 del Regolamento indichi come autorità competenti la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico, si rivela necessaria una lettura conforme alle modifiche apportate dal d.l. 82 del 2021: perciò, l’autorità competente diventerà l’ACN.

L’ultimo provvedimento attuativo del Perimetro, al momento mancante, assumerà anch’esso la forma di un d.P.C.M. e sarà deputato a fissare i criteri in base ai quali il CVCN potrà accreditare e avvalersi di laboratori di supporto per l’espletamento delle proprie funzioni di verifica sulla sicurezza dei beni, servizi e sistemi ICT di cui i soggetti inclusi nel Perimetro intendono servirsi attraverso specifiche procedure di affidamento. L’approvazione di tale provvedimento è attesa entro l’autunno.

Provvedimenti attuativi del d.l. 105/2019

d.P.C.M. 30 luglio 2020, n. 131 – Regolamento in materia di Perimetro di sicurezza nazionale cibernetica

Perimetro di sicurezza nazionale → si applica a:

si applica a:

- Soggetti che esercitano una funzione essenziale dello Stato
  - Soggetti a cui l'ordinamento attribuisce compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti (art. 2, comma 1, lett. a).
- Soggetti, pubblici o privati, che prestano un servizio essenziale per gli interessi dello Stato
  - Soggetti che pongono in essere attività: 1. strumentali all'esercizio di funzioni essenziali dello Stato; 2. necessarie per l'esercizio e il godimento dei diritti fondamentali; 3. necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; 4. di ricerca; 5. relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove prestino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo economico nazionale (art. 2, comma 1, lett. b).

Operanti nei seguenti settori di attività: a) governativo nell'ambito delle amministrazioni CISR; b) interno; c) difesa; d) spazio e aerospazio; e) energia; f) telecomunicazioni; g) economia e finanza; h) trasporti; i) servizi digitali; l) tecnologie critiche di cui al reg. (UE) 2019/452; m) enti e previdenziali/lavoro.

L'esercizio delle loro funzioni o dei loro servizi essenziali dipende da reti, sistemi o servizi informatici la cui compromissione può arrecare un pregiudizio per la sicurezza nazionale.

Per valutare la sussistenza di tale pregiudizio, si tiene conto dei seguenti effetti: 1. estensione territoriale; 2. numero e la tipologia di utenti potenzialmente interessati; 3. livelli di servizio garantiti; 4. possibili ricadute economiche; 5. perdita delle disponibilità, integrità o riservatezza dei dati e delle informazioni trattate, avuto riguardo della loro tipologia, quantità, finalità e sensibilità; 6. continuità del servizio; 7. tempo di ripristino.

Predispongono e aggiornano, almeno annualmente, l'elenco dei beni ICT necessari a svolgere la funzione o il servizio essenziale, tramite una valutazione basata sul rischio che tenga conto: 1. dell'impatto dell'incidente sul bene ICT, in termini di compromissione, disponibilità, integrità o riservatezza dei dati e delle informazioni da esso trattati; 2. delle dipendenze con altre reti, sistemi, servizi informatici o infrastrutture fisiche di altri soggetti.

d.P.C.M. 25 novembre 2020 – Elenco dei soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica

- Lista degli attori nazionali, pubblici o privati, soggetti alle regole del Perimetro
  - Formata da oltre 100 soggetti
    - A ciascuno viene data, separatamente, comunicazione dell'avvenuta iscrizione
  - Elenco non soggetto a pubblicazione
  - Escluso il diritto di accesso
  - Adottata dal Presidente del Consiglio dei Ministeri su proposta del CISR
  - Operativa a partire dal 23 giugno 2021

d.P.C.M. 15 giugno 2021 – Aggiornamento dell'elenco dei soggetti inclusi nel Perimetro di sicurezza nazionale cibernetica

- Allargamento della lista degli attori, pubblici o privati, soggetti alle regole del Perimetro
- Complessivamente, i soggetti inclusi nella lista esercitano 223 funzioni essenziali o comunque prestano un servizio essenziale per gli interessi civili, sociali o economici dello Stato

d.P.C.M. 14 aprile 2021, n. 81 (pubblicato in GU l'11 giugno 2021) – Regolamento in materia di notifiche degli incidenti e di misure volte a garantire elevati livelli di sicurezza

Soggetti inclusi nel Perimetro

notificano

- **l'incidente** avente impatto sui beni ICT di propria pertinenza al CSIRT, che trasmette la notifica ricevuta a:
  - **DIS**, che a sua volta inoltra la notifica a:
    - **MISE** — per i soggetti privati inclusi nel Perimetro
    - **Presidenza del Consiglio dei Ministri - MITD** — per i soggetti pubblici inclusi nel Perimetro
  - **Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione**
  - **Autorità NIS** — se i notificanti sono anche soggetti alla Direttiva NIS (OSE e FSD)

entro sei ore / **entro un'ora** dal momento in cui i soggetti inclusi nel Perimetro sono venuti a conoscenza dell'incidente

- se → **Incidente meno grave (Tabella 1, All. A)**
  Esempio:
  - Infezione
  - Perdita di confidenzialità o integrità
  - Perdita e/o corruzione di dati
- se → **Incidente più grave (Tabella 2, All. A)**
  Esempio:
  - Inibizione delle funzioni di risposta
  - Compromissione dei processi di controllo
  - Disservizio intenzionale
  - Divulgazione non autorizzata di dati digitali

tempestivamente …in materia di notifiche

- la rilevazione di eventi comunque correlati all'incidente (art. 3, c. 5)
- il piano di attuazione delle attività di ripristino dei beni ICT impattati dall'incidente oggetto di notifica (art. 3, c. 8)

salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa

<u>Incidente</u>: ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziale, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei sistemi informatici (art. 1, c. 1, lett. h))

<u>Impatto</u>: limitazione della operatività del bene ICT ovvero compromissione della disponibilità, integrità o riservatezza dei dati e delle informazioni da esso trattati ai fini dello svolgimento della funzione o del servizio essenziale (art. 1, c. 1, lett. i))

può chiedere al notificante:
- un aggiornamento della notifica (art. 3, c. 7)
- una relazione tecnica sugli elementi significativi dell'incidente, tra cui le conseguenze dell'impatto sui beni ICT derivanti dall'incidente e le azioni intraprese per porvi rimedio (art. 3, c. 8)

- Il sistema di notificazione degli incidenti diventa operativo a partire dal 1° gennaio 2022. Prima di tale data, i soggetti già inclusi nel Perimetro procedono alle notifiche in via sperimentale.
- È anche previsto un sistema di notificazione su base volontaria (art. 4).
- Quando i soggetti inclusi nel Perimetro sono anche OSE o FDS (come individuati dal d.lgs. 65/2018), la notifica dell'incidente al CSIRT costituisce anche adempimento ai sensi della Direttiva NIS.

d.P.C.M. 14 aprile 2021, n. 81 (pubblicato in GU l'11 giugno 2021) – Regolamento in materia di notifiche degli incidenti e di misure volte a garantire elevati livelli di sicurezza

…in materia di misure di sicurezza

Soggetti inclusi nel Perimetro

adottano

misure di sicurezza

per ciascun bene ICT di propria pertinenza

e ne danno tempestiva comunicazione al

DIS

Rende tempestivamente disponibili le comunicazioni ricevute a

Presidenza del Consiglio dei Ministri - MITD

per i soggetti pubblici inclusi nel Perimetro

per i soggetti privati inclusi nel Perimetro

MISE

Svolgono attività di verifica e controllo sull'adeguatezza delle misure adottate

Se si procede all'aggiornamento dell'elenco, contestualmente occorre valutare se sia necessario adeguare le misure di sicurezza. In caso affermativo, si provvede all'adeguamento e se ne dà comunicazione entro trenta o sei mesi in base alla natura della misura di sicurezza adottata (art. 8, c. 4)

indicati nell'elenco trasmesso a

entro trenta mesi

entro sei mesi

dalla data di trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici di loro pertinenza, dal cui malfunzionamento, interruzione ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale

se

se

Misure di sicurezza più complesse (appartenenti alla categoria B di cui all'appendice 2 dell'allegato B)

Esempio:
PR.DS-1: i dati digitali trattati mediante l'impiego di beni ICT, la cui compromissione sotto il profilo della disponibilità, integrità e riservatezza può avere un impatto sulla sicurezza nazionale, sono conservati, elaborati ovvero estratti esclusivamente mediante l'impiego di infrastrutture fisiche e tecnologiche, anche se esternalizzate, localizzate nel territorio nazionale.

Misure di sicurezza meno complesse (appartenenti alla categoria A di cui all'appendice 2 dell'allegato B)

Esempio:
RS.CO-1: il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente

devono essere applicate dai soggetti inclusi nel Perimetro entro sessanta giorni dall'entrata in vigore del decreto

Misure minime di sicurezza per tutela delle informazioni (art. 9)

volte a tutelare le informazioni relative all'elenco dei soggetti inclusi nel Perimetro, all'elenco dei beni ICT e agli elementi delle notifiche degli incidenti

Sono suddivise in due categorie:
1. misure di sicurezza relative ai trattamenti svolti con l'ausilio di strumenti elettronici
2. misure di sicurezza fisica e documentale

d.P.R. 5 febbraio 2021, n. 54 (pubblicato in GU il 23 aprile 2021) – Regolamento in materia di valutazione e verifica degli acquisti ICT

… in materia di procedura di valutazione del CVCN e dei CV

Soggetti inclusi nel Perimetro

danno comunicazione dell'intenzione di acquisire

uno dei beni, sistemi o servizi ICT

appartenenti a determinate categorie individuate da un apposito d.P.C.M. (in attesa di adozione) sulla base dei criteri di cui all'art. 13

al Centro di valutazione e certificazione nazionale – CVCN — istituito presso il MISE

o

ai Centri di valutazione - CV — di cui possono avvalersi il Ministero della Difesa e il Ministero degli Interni per i settori strategici di loro competenza

prima dell'avvio delle procedure di affidamento ovvero, ove non previste, prima della conclusione di contratti relativi alla fornitura di beni, sistemi e servizi ICT, dal cui malfunzionamento, interruzione o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale

anche nel caso in cui le procedure siano espletate attraverso centrali di committenza (per es. Consip S.p.A.)

La comunicazione include (art. 3, c. 4 e 5):

- i dati identificativi del soggetto incluso nel Perimetro;
- la descrizione generale dell'oggetto della fornitura;
- la categoria di appartenenza dell'oggetto della fornitura;
- le informazioni relative all'eventuale acquisizione mediante gli strumenti di acquisto e di negoziazione di Consip S.p.A. o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti;
- il documento di analisi del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego

Analisi del rischio: un processo che consente di identificare i fattori di rischio di un incidente, valutandone la probabilità e l'impatto potenziale sulla continuità, sulla sicurezza o sulla efficacia della funzione essenziale o del servizio essenziale, e conseguentemente di trattare tale rischio individuando ed implementando idonee misure di sicurezza (art. 1, lett. g)).

avviano un procedimento di verifica e valutazione dell'analisi documentale ricevuta che si articola in tre fasi:

1. verifiche preliminari

consistono ne:
- la richiesta di informazioni,
- l'instaurazione di una collaborazione con il fornitore (art. 5, c.),
- l'individuazione dei test da eseguire.

2. preparazione test

se l'oggetto di fornitura è stato sottoposto a precedenti valutazioni o è in corso di valutazione, sono effettuate una serie di verifiche finalizzate ad evitare la duplicazione di test già eseguiti (art. 6, c., lett. a), e c. 2)

se l'oggetto di fornitura non è stato sottoposto a precedenti valutazioni o non sia in corso di valutazione, in collaborazione con il soggetto incluso nel Perimetro vengono identificati i test da eseguire (art. 6, c., lett. b), c. 3 e 4)

da eseguire nel termine di 45 giorni dalla comunicazione (prorogabili di altri 15 nei casi di particolare complessità): decorso inutilmente tale termine i soggetti proseguono la procedura di affidamento o l'esecuzione del contratto

3.esecuzione test

i test vengono eseguiti presso i laboratori (interni) del CVCN, dei CV o quelli (esternalizzati) dei LAP (laboratori accreditati di prova) ovvero dal di loro personale presso il soggetto incluso nel Perimetro o il fornitore (entro 60 dì dalla messa a disposizione dell'oggetto di valutazione)

viene redatto un rapporto di prova nel quale sono indicati l'ambiente del test, le prove eseguite e i relativi esiti:

all'esito delle verifiche, possono definire con apposito provvedimento le condizioni, i test da eseguire e le clausole sospensive o risolutive da inserire nei bandi di gara o nei contratti

Esito positivo: eventualmente rafforzato da prescrizioni di utilizzo dell'oggetto di affidamento

Esito negativo: vengono comunicati i motivi ostativi all'affidamento

d.P.R. 5 febbraio 2021, n. 54 (pubblicato in GU il 23 aprile 2021) – Regolamento in materia di valutazione e verifica degli acquisti ICT

… in materia di criteri tecnici per l'individuazione delle categorie di acquisti ICT oggetto di valutazione

Le categorie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN o dai CV sono individuate da un apposito d.P.C.M. (d.P.C.M. del 15 giugno 2021) sulla base dell'esecuzione o svolgimento delle seguenti funzioni (art. 13):

a) commutazione oppure protezione da intrusioni e rilevazione di minacce informatiche in una rete, ivi inclusa l'applicazione di politiche di sicurezza;
b) comando, controllo e attuazione in una rete di controllo industriale;
c) monitoraggio e controllo di configurazione di una rete di comunicazione elettronica;
d) sicurezza della rete riguardo alla disponibilità, autenticità, integrità o riservatezza dei servizi offerti o dei dati conservati, trasmessi o trattati;
e) autenticazione e allocazione delle risorse di una rete di comunicazione elettronica;
f) implementazione di un servizio informatico per mezzo della configurazione di un programma software esistente oppure dello sviluppo, parziale o totale, di un nuovo programma software, costituente la parte applicativa rilevante ai fini dell'erogazione del servizio informatico stesso.

d.P.R. 5 febbraio 2021, n. 54 (pubblicato in GU il 23 aprile 2021) – Regolamento in materia di valutazione e verifica degli acquisti ICT

Presidenza del Consiglio dei Ministri - MITD
per i soggetti pubblici inclusi nel Perimetro

MISE
per i soggetti privati inclusi nel Perimetro

Strutture specializzate – Amministrazioni Forze di polizie e Forze armate
per i beni ICT connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato

dispongono

… in materia di ispezioni e verifiche

al fine di accertare l'adempimento da parte dei soggetti inclusi nel Perimetro dei seguenti obblighi (art. 14, c. 1):

a) predisposizione, aggiornamento e trasmissione dell'elenco dei beni ICT dal cui malfunzionamento, interruzione ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale;
b) notifica al CSIRT degli incidenti aventi impatto sui beni ICT nei termini e nei modi previsti dal d.P.C.M n. 81 del 2021;
c) adozione di idonee misure di sicurezza nei termini e nei modi previsti dal d.P.R. 54 del 2021;
d) comunicazione al CVCN (o ai CV) dell'intenzione di acquisire beni ICT nei termini e nei modi previsti dal d.P.R. 54 del 2021;
e) impiego di beni ICT in conformità alle condizioni e con superamento dei test imposti dal CVCN (o dai CV);
f) collaborazione per l'effettuazione di tali test;
g) osservanza delle prescrizioni formulate all'esito delle attività di verifica e ispezione;
h) osservanza delle prescrizioni di utilizzo fornite dal CVCN (o dai CV).

verifiche

Attività di analisi e controllo documentale delle evidenze e di ogni altro elemento di fatto e diritto (art. 17)

Si devono concludere entro 120 giorni dalla data di comunicazione dell'avvio del relativo procedimento

Delle attività svolte viene redatto apposito verbale (sottoscritto anche dal referente del soggetto controllato in caso di ispezione).

ispezioni

Attività di tipo ricognitivo e valutativo, consistenti nel riscontro delle evidenze eventualmente acquisite in sede di verifica ovvero nell'analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto ritenuti necessari (art. 18)

Si concludono entro 90 giorni dalla data di comunicazione dell'avvio del relativo procedimento

L'avvio del procedimento è preceduto da un'informativa in cui sono riportate: le date e i siti dell'ispezione, le persone da intervistare, i beni ICT da ispezionare, i nominativi degli ispettori e ogni altra informazione utile (art. 18, c. 3)

I soggetti ispezionati devono fare il possibile per agevolare l'ispezione (art. 18, c. 7)

e, richiedendo le informazioni e la documentazione necessarie, comunicano l'avvio dei relativi procedimenti ai soggetti inclusi nel perimetro, i quali…

nominano un incaricato in possesso di professionalità e di competenze nella materia della sicurezza cibernetica, quale unico referente per lo svolgimento dell'attività

Raccolti gli esiti delle attività, adottano e comunicano il provvedimento di conclusione del procedimento, impartendo (ove necessario) specifiche prescrizioni

Nei casi previsti, viene avviato il procedimento per l'applicazione delle sanzioni amministrative previste dall'art. 1, c. 9, del d.l. 105 del 2019

Esempio:
Il mancato adempimento dell'obbligo di notifica dell'incidente nei termini prescritti è punito con la sanzione amministrativa pecuniaria da euro 250.00 a euro 1.800.000.

d.P.C.M. 15 giugno 2021 (pubblicato in GU il 19 agosto 2021) – Elenco dei beni, servizi e sistemi ICT oggetto di valutazione del CVCN

I soggetti inclusi nel Perimetro devono comunicare al CVCN o ai CV la loro intenzione di procedere (anche per il tramite di centrali di committenza) all'affidamento di forniture di beni, sistemi e servizi ICT se tali beni, sistemi e servizi appartengono a una delle categorie individuate dal Presidente del Consiglio dei Ministri in un apposito elenco aggiornato con cadenza almeno annuale.

L'attuale elenco individua quattro categorie:

1. Componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione)
2. Componenti hardware e software che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati
3. Componenti hardware e software per acquisizione dati, monitoraggio, supervisione, controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali
4. Applicativi software per l'implementazione di meccanismi di sicurezza

d.P.C.M. _____ criteri di accreditamento dei laboratori di cui il CVCN può avvalersi per l'esercizio delle sue funzioni (in attesa di definizione)

6. *Le varianti in corso d'opera: l'Agenzia per la Cybersicurezza Nazionale e la gestione del Perimetro (d.l. 82/2021)*

In chiusura, è doveroso ancora qualche riferimento al più volte richiamato d.l. 82 del 2021. Infatti, oltre ad occuparsi delle funzioni dell'ACN, il decreto istituisce altri due nuovi organi.

In primo luogo, ex art. 4 del d.l. 82 del 2021, accanto al Comitato interministeriale per la sicurezza della Repubblica viene creato un apposito comitato dedicato alla cybersecurity: il Comitato interministeriale per la cybersicurezza. Quest'ultimo, in virtù della sua specificità, sostituirà il primo in tutte le attività di supporto alle politiche della Presidenza del Consiglio dei ministri nell'ambito del Perimetro di sicurezza, ad esempio attraverso la formulazione di pareri per la definizione dei d.P.C.M. di attuazione della materia. Inoltre, svolgerà funzioni di sorveglianza sull'attuazione della strategia nazionale di cybersicurezza, indicando al Presidente del Consiglio gli opportuni indirizzi generali.

Ai sensi dell'art. 8 del d.l. 82 del 2021, viene poi istituito il Nucleo per la cybersicurezza, il quale coadiuverà il Presidente del Consiglio dei ministri in materia di prevenzione e preparazione a eventuali crisi "cyber". L'obiettivo verrà perseguito attraverso la pianificazione di operazioni di risposta alle crisi e la predisposizione di esercitazioni, anche sulla base dei dati delle segnalazioni acquisiti dal CSIRT nel corso del tempo.

Decreto-legge 82/2021

Obiettivi

- Adeguare le strategie di cybersicurezza al fine di rendere il Paese più sicuro e resiliente, rafforzando la fiducia dei cittadini
- Sviluppare e coordinare capacità avanzate tese ad assicurare l'intero ciclo della cyber-resilienza
- Razionalizzare e concentrare le competenze in materia di cybersicurezza
- Attuare il Piano Nazionale di Ripresa e Resilienza, deliberato dal CdM nella riunione del 29 aprile 2021, che pone la cybersicurezza a fondamento della trasformazione digitale della PA

Oggetto

- Definizione delle competenze della Presidenza del Consiglio dei Ministri in materia di cybersicurezza
- Istituzione del Comitato interministeriale per la cybersicurezza, dell'Agenzia per la cybersicurezza nazionale e del Nucleo per la cybersicurezza
- Gestione delle crisi di natura cibernetica
- Ridefinizione dell'architettura nazionale cyber, con particolare riferimento agli ambiti:
  a. della sicurezza delle reti e dei sistemi informativi (NIS);
  b. del Perimetro di sicurezza nazionale cibernetica;
  c. della sicurezza delle comunicazioni elettroniche (TELCO).

Definizioni

Cybersicurezza: l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità, e garantendone altresì la resilienza (art., c. 1, lett. a)).

Competenze esclusive del Presidente del Consiglio dei Ministri – art. 2

Il Presidente del Consiglio dei Ministri

- Assume l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.
- Adotta la strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza nazionale.
- Nomina e revoca il direttore generale e il vicedirettore generale dell'Agenzia per la cybersicurezza nazionale, previa informazione al presidente del COPASIR.

Istituzione e funzioni del Comitato interministeriale per la cybersicurezza (CIC) – art. 4

CIC

Istituito presso la Presidenza del Consiglio

È composto da:
- il Presidente del Consiglio;
- l'Autorità delegata dal PdC (ove istituita);
- il Ministro degli esteri;
- il Ministro degli interni;
- il Ministro della giustizia;
- il Ministro della difesa;
- il Ministro dell'economia;
- il Ministro dello sviluppo economico;
- il Ministro della transizione ecologica;
- il Ministro dell'università e della ricerca;
- il Ministro delegato all'innovazione tecnologica;
- il Ministro dei trasporti;
- il Direttore generale dell'Agenzia per la cybersicurezza nazionale (segretario)

- Propone al Presidente del Consiglio gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale.
- Esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza.
- Promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti interessati alla cybersicurezza, nonché alla 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 nella medesima materia.
- Esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale.
- Svolge le funzioni già attribuite al CISR all'interno del Perimetro di sicurezza nazionale cibernetica, fatta eccezione per quelle attribuite nei casi di crisi cibernetica (v. art. 5 d.l. 105/2019 e d.P.C.M. 17 febbraio 2017).

tecniche normative **Istituzione e funzioni dell'Agenzia per la cybersicurezza nazionale** – artt. 5, 6 e 7

Agenzia per la cybersicurezza nazionale

- Ha sede a Roma.
- Ha personalità giuridica di diritto pubblico.
- È dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria.

Organi:
- Direttore e vicedirettore generale (mandato di durata quadriennale rinnovabile una sola volta)
- Collegio dei revisori dei conti

Consulta il Garante Privacy e collabora con esso anche in relazione agli incidenti che comportano violazioni di dati personali (art. 7, c.5).

- Assicura il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche del Paese (art. 7, c. 1, lett a)).
- Predispone la strategia nazionale di cybersicurezza (lett. b)).
- Svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza (lett. c)).
- È l'Autorità nazionale competente e Punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi per le finalità di cui al d.lgs. 65/2018 attuativo della cd. Direttiva NIS, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo d.lgs. 65/2018 (lett. d)).
- È l'Autorità nazionale di certificazione della cybersicurezza ai sensi del cd. Cybersecurity Act e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al MISE, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni (lett. e)).
- Assume tutte le funzioni in materia di cybersicurezza già attribuite al MISE, comprese quelle relative (lett. f)):
  - al Perimetro di sicurezza nazionale cibernetica, ivi incluse le funzioni attribuite al CVCN;
  - alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui al d.lgs. 259/2003;
  - alla sicurezza delle reti e dei sistemi informativi, di cui al d.lgs. 65/2018.
- Assume tutte le funzioni attribuite alla Presidenza del Consiglio dei Ministri e al DIS in materia di Perimetro di sicurezza nazionale cibernetica (lett. h) e i)).
- Assume tutte le funzioni in materia di cyberisicurezza già attribuite all'AGID (lett. m)).
- Sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CISRT (lett. n)).
- Partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese (lett. o)).
- 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 internazionali. A tal fine, esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza (lett. p)).
- Coordina, in raccordo con il Ministero degli esteri, la cooperazione internazionale in materia di cybersicurezza e, a livello eurounitario cura i rapporti con i competenti organismi, istituzioni ed enti (lett. q)).
- Assicura il coinvolgimento di soggetti pubblici e privati nazionali, anche sulla base di apposite convenzioni, per la formazione, la ricerca, lo sviluppo di competenze e la promozione della consapevolezza in materia di cybersicurezza (lett. r), s), t), u), v), z)).
- È designata come Centro nazionale di coordinamento ai sensi del reg. (UE) 2021/887, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca (lett. aa)).

Istituzione e funzioni del Nucleo per la cybersicurezza – artt. 8, 9 e 10

Nucleo per la cybersicurezza

È costituito in via permanente presso l'Agenzia per cybersicurezza nazionale.

È presieduto dal direttore generale dell'Agenzia (o dal vice designato).
È composto da:
- il Consigliere militare del Presidente del Consiglio;
- un rappresentante de:
  - il DIS, l'AISE e l'AISI;
  - il Ministero degli esteri;
  - il Ministero degli interni;
  - il Ministero della giustizia;
  - il Ministero della difesa;
  - il Ministero dell'economia;
  - il Ministero dello sviluppo economico;
  - il Ministero della transizione ecologica;
  - il Ministero dell'università e della ricerca;
  - il Ministero delegato all'innovazione tecnologica;
  - il Dipartimento di protezione civile.

In situazioni di crisi cibernetica, in ragione della necessità, è integrato da rappresentanti di altri Ministeri o Dipartimenti.

Supporta il Presidente del Consiglio dei Ministri nella materia della cybersicurezza per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento (art. 8, c. 1). In particolare (art.9):

- Formula proposte di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale.
- Promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile.
- Promuove e coordina lo svolgimento di esercitazioni interministeriali ovvero la partecipazione a esercitazioni internazionali.
- Valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della cybersicurezza, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi.
- Riceve, per il tramite del CSIRT, le comunicazioni circa i casi significativi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità delle reti e dei servizi.
- Riceve dal CSIRT le notifiche di incidenti.
- Valuta se le violazioni e gli incidenti comunicati dal CSIRT assumono la dimensione di "situazione di crisi cibernetica".

<u>Situazione di crisi cibernetica</u>: situazione in cui l'evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale tale da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria ma con l'assunzione di decisioni coordinate in sede interministeriale (art. 2, c. 1., lett. o del d.P.C.M. 17 febbraio 2017).

Supporta il Presidente del Consiglio dei Ministri in materia di gestione di situazioni di crisi di natura cibernetica (art. 10). In particolare:

- Assicura il coordinamento tra le attività di reazione e stabilizzazione di competenza delle diverse amministrazioni e le determinazioni del Presidente del Consiglio.
- Mantiene costantemente aggiornato il Presidente del Consiglio sulla crisi in atto e raccoglie tutti i dati relativi alla crisi.
- Elabora rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati.
- Partecipa ai meccanismi europei di gestione delle crisi, assicurando altresì collegamenti con gli omologhi organismi di altri Stati, della NATO, dell'UE o di organizzazioni internazionali di cui l'Italia fa parte.

7. *I prossimi appuntamenti normativi: una previsione (provvedimenti attuativi del d.l. 82/2021)*

A fronte del quadro normativo così schematizzato non resta che constatare come la disciplina della cibersicurezza nazionale si trovi ancora in una fase di costruzione.

Non solo mancano gli ultimi provvedimenti attuativi del Perimetro di sicurezza, ma – a seguito dell'entrata in vigore del d.l. 82/2021 – ora il Governo è anche chiamato ad adottare tutti gli strumenti necessari al funzionamento della neonata Agenzia per la cybersicurezza nazionale.

A quest'ultimo proposito, senza alcuna presunzione di completezza, è possibile qui teorizzare brevemente una scansione di quelli che saranno i futuri atti esecutivi del d.l. 82/2021.

Innanzitutto, l'organizzazione e il funzionamento dell'ACN dovranno essere definiti da un apposito regolamento da approvare mediante d.P.C.M. entro centoventi giorni dalla data di entrata in vigore della legge di conversione del decreto, in base a quanto disposto dall'art. 11, c. 3, del d.l. 82 del 2021.

In secondo luogo, secondo le stesse tempistiche, dovranno essere emanati due regolamenti in merito alla contabilità e alle disposizioni finanziarie dell'ACN. Il primo si occuperà della sua autonomia gestionale e contabile, ex art. 11, c. 3, del d.l. 82 del 2021, mentre il secondo determinerà le procedure per la stipula dei contratti e degli appalti di lavori e forniture di beni e servizi, e per le attività finalizzate alla tutela della sicurezza nazionale nello spazio cibernetico, ex art. 11, c. 4, del d.l. 82 del 2021.

In terzo luogo, a norma dell'art. 12 del medesimo decreto, dovrà essere affrontata la regolamentazione del contingente di personale dell'ACN, in relazione all'ordinamento, al reclutamento e al trattamento previdenziale. In via residuale, potrà anche essere fatto utilizzo di apposito personale presso il Ministero della difesa. Questa possibilità però necessiterà di un apposito d.P.C.M. per la definizione dei rispettivi rapporti.

Infine, considerato che l'Agenzia svolgerà funzioni fra loro molto eterogenee, il decreto prevede che presso la stessa dovrà costituirsi un comitato tecnico-scientifico, formato anche da rappresentanti (designati mediante d.P.C.M.) dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza. Fra le diverse attività demandante al comitato, vi è anche quella di promuovere la formazione delle risorse umane: in tal caso si potrà ricorrere alle strutture formative e alle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno. Anche in questo caso, i rapporti con i Ministeri dovranno essere regolati mediante d.P.C.M..

8. *Conclusioni*

Dalla ricostruzione offerta mediante gli schemi contenuti nel presente contributo emerge come negli ultimi anni la materia della sicurezza informatica abbia assunto un interesse sempre più crescente in capo al legislatore europeo e, soprattutto, nazionale.

Ciò rappresenta l'esito di una maggiore consapevolezza che è maturata attorno al tema a causa dell'innegabile e notevole incremento – sia in termini di numeri che di complessità – degli attacchi "cyber" rilevati.

Questa consapevolezza si è tradotta in interventi volti a costruire un'elevata protezione dello Stato sotto il versante digitale. È nata perciò la necessità di dare una nuova forma alla difesa degli interessi strategici nazionali.

La prima a muoversi in questa direzione è stata l'Unione europea, che – abbandonata l'era delle raccomandazioni e degli atti non vincolanti – ha avviato un percorso per dar vita ad un sistema con un buon livello di armonizzazione, nell'ottica di un serio rafforzamento della propria posizione internazionale, ma anche di una migliore tenuta e apertura del mercato dei servizi e dei nuovi beni digitali. La cybersecurity, infatti, al pari della protezione dei dati personali, è un essenziale prerequisito per il libero godimento della libera circolazione in tutte le sue forme.

Proprio sotto l'impulso del diritto eurounitario si è quindi mosso il legislatore (e, soprattutto, il Governo) italiano, iniziando a erigere i pilastri normativi su cui si regge l'attuale sicurezza cibernetica del Paese.

Come anticipato, la disciplina nazionale vive ancora una fase di costruzione, ma la strada ormai appare sufficientemente tracciata, grazie all'approvazione dei decreti-legge n. 105 del 2019 e n. 82 del 2021. Pertanto, non rimane che attendere l'approvazione degli ultimi provvedimenti esecutivi previsti da tali decreti per vedere l'attuale quadro normativo completo.

Anche se resta un dato non trascurabile. La tecnologia digitale è in rapidissima evoluzione e ciò costringerà certamente l'ordinamento a effettuare senza soluzione di continuità interventi di consolidamento e rafforzamento dell'intero sistema normativo di riferimento. Non si può perciò escludere che nel giro di pochi anni "il tempio" della sicurezza cibernetica nazionale possa anche assumere un'architettura ben diversa da quella mostrata oggi.