MISSIONE 1 – COMPONENTE 1 – LA CYBERSICUREZZA NELL'ORDINAMENTO ITALIANO

PNRR

Dossier

Sommario

Capitolo I: La Cybersicurezza e le minacce informatiche

1.1 La Cybersicurezza

La *cybersicurezza* può essere definita come *l'insieme di mezzi, tecnologie, attività e procedure teso a garantire la sicurezza informatica dei computer, server, dispositivi mobili, sistemi elettronici, reti informatiche (con particolare attenzione alla rete internet) in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici*. Essa, quindi, è riferita all'insieme di tecnologie, processi e procedure finalizzate alla protezione di reti, dispositivi, programmi e dati da attacchi, danni o accessi non autorizzati.

La necessità di garantire la sicurezza di reti e sistemi informatici emerge in tutta la sua urgenza ove si tenga conto del fatto che la pubblica amministrazione e le organizzazioni private raccolgono, elaborano e archiviano sui propri dispositivi una quantità sempre maggiore di dati, con precisione sempre più capillare e, a tal fine, utilizzano reti e altre infrastrutture (es. la *Piattaforma Digitale Nazionale Dati*) che permettono la trasmissione e la condivisione dei dati in proprio possesso con altri soggetti istituzionali (come nel caso della c.d. *cooperazione applicativa*).

Più in generale, a fronte della crescita esponenziale dell'importanza della rete in molteplici attività umane[1] corrisponde un analogo incremento della quantità e della qualità dei dati *on-line* molti dei quali sensibili o strettamente riservati (es. informazioni sanitarie o personali, dati genetici, dati biometrici, dati finanziari, ecc.).

L'accesso non autorizzato a tali dati, la loro esposizione senza il previo consenso, la loro alterazione o distruzione sono tutti eventi in grado di dare vita a conseguenze negative per il titolare dei dati stessi.

Purtroppo, l'esperienza comune ci insegna che la "crescita" della rete è stata accompagnata da un analogo incremento ed una continua evoluzione delle minacce in essa presenti[2]. È divenuta, dunque, sempre più impellente **la necessità di una tutela efficace contro le minacce e gli attacchi di *hacker*** e malintenzionati in genere e, quindi, di un rafforzamento dei sistemi di sicurezza che coinvolga strumenti, procedure e professionalità adeguate.

[1] La tendenza verso una sempre maggiore importanza della rete nella società odierna appare sostenuta da due impulsi fondamentali. Da un lato la crescita costante del numero di utenti e, dall'altro, l'incremento del numero dei dispositivi connessi (PC, *tablet*, *smartphone*, *smart* TV, ecc.). Quest'ultimo aspetto sembra destinato ad una crescita sempre maggiore grazie alle nuove frontiere della *domotica* e del c.d. *internet delle cose*.

[2] Le tecniche utilizzate per portare a segno attacchi *cyber* sono divenute, infatti, sempre più raffinate ed all'avanguardia, al punto da essere in grado, in molti casi, di superare o aggirare i sistemi e le procedure di sicurezza implementate proprio per contrastarle.

I settori maggiormente colpiti dagli attacchi criminali sono: i servizi bancari, i servizi medici, i rivenditori e gli enti pubblici. Qualunque dispositivo proiettato sulla rete è, però, potenzialmente esposto a rischio di attacchi *cyber*.

1.2. Le diverse tipologie di attacchi informatici

Schematicamente possiamo indicare tre diversi tipi di comportamenti illegali:

1. **Cybercrimine**: attività sanzionate dall'ordinamento penale, poste in essere per mezzo (e spesso con l'abuso) delle tecnologie dell'informazione e della comunicazione[3] (sia *hardware* che software) orientate contro i beni informatici[4].
2. **Cyberattacchi**: azioni, manovre o tentativi posti in essere da individui singoli o organizzazioni verso sistemi informatici, infrastrutture, reti di calcolatori e/o dispositivi elettronici con la finalità di raccogliere, alterare o distruggere dati e informazioni[5];
3. **Cyberterrorismo**: attacchi illegali e minacce rivolti contro sistemi informativi di organizzazioni nazionali messi in atto per intimidire o costringere un governo o il suo popolo ad un dato comportamento o per ingenerare paura e disorientamento nella società e perseguire, così, obiettivi politici e/o sociali[6].

[3] Il *cybercrimine* è materia disciplinata dal diritto penale che nel corso del tempo ne ha delineato lo scenario – anche in funzione dell'evoluzione tecnologica e del consolidamento di tecniche criminali sempre più raffinate – sia individuando nuove figure criminose sia riconducendo i comportamenti in rete a figure criminose già esistenti (ad es. l'accesso abusivo ad un sistema informatico che è stato assimilato al reato di violazione di domicilio di cui all'art. 614 del Codice penale). Nello scenario attuale i crimini informatici più diffusi consistono in aggressioni mirate a sistemi aziendali o istituzionali, finalizzati al conseguimento di un vantaggio economico o a provocare l'interruzione di un dato servizio o un'attività aziendale.

[4] Pertanto, sono considerati reati informatici sia la frode o il furto di informazioni riservate realizzate grazie all'utilizzo di dispositivi digitali, sia il danneggiamento di sistemi informatici.

[5] Le motivazioni alla base degli attacchi informatici possono essere ricondotte essenzialmente a tre categorie principali: *politica*, *criminale* e *personale*. Gli attacchi a sfondo politico sono perpetrati da organizzazioni che intendono sfruttare l'evento per attirare l'attenzione sulle cause portate avanti e quindi, essenzialmente, per avere visibilità. Le aggressioni di tipo criminale sono, invece, finalizzate al conseguimento di facili guadagni finanziari grazie al furto di denaro, al furto di dati (incluso lo spionaggio industriale) o al danneggiamento o all'interruzione dell'attività di concorrenti commerciali. Le aggressioni animate da motivazioni personali sono riferibili a soggetti che hanno particolari legami con l'organizzazione colpita (es. dipendenti, ex dipendenti, utenti, ecc.) e possono avere motivazioni piuttosto varie che vanno dalla ricerca di profitti illeciti (furto di dati o di denaro), al mero risentimento (come nel caso di danneggiamenti fini a sé stessi).

[6] Gli atti di *cyberterrorismo* si caratterizzano per la loro attitudine a provocare violenza o a mettere in pericolo persone o beni, provocando danni sufficienti ad ingenerare sentimenti di paura (es. attacchi che determinano esplosioni, incidenti aerei, contaminazione delle condotte idriche acqua, gravi perdite economiche, ecc.).

1.2.1 I Malware

La minaccia informatica più comune e più diffusa in campo informatico è rappresentata dai *malware*[7]. Con tale termine si intende, genericamente, un programma o un codice dannoso che mette a rischio un sistema informatico danneggiandolo o provocandone il malfunzionamento, che si diffonde, normalmente attraverso la diffusione di allegati e-mail non richiesti o *download* in apparenza legittimi[8].

I *malware* non sono in grado arrecare danni fisici alle componenti *hardware* dei dispositivi ma, intervenendo sulla componente *software*, possono compromettere le funzioni fondamentali di un terminale (computer, tablet, *smartphone*, ecc.) o spiare le attività degli utenti o, infine, rubare, criptare o eliminare dati.

L'utilizzo dei *malware* è, quindi, finalizzato ad invadere, danneggiare o disattivare reti, sistemi, e terminali, assumendone parzialmente il controllo. Per questa via i criminali informatici mirano ad ottenere vantaggi (economici o di altro tipo) a danno degli utenti.

Le tipologie di *malware* più comuni sono:

- **Virus:** *software malevolo* in grado di replicarsi autonomamente e non rilevabile dall'utente, che infetta uno o più *file* residenti sul sistema attaccato, integrandosi nei codici eseguibili e/o nel sistema operativo del sistema informatico aggredito[9];
- **Worm**: *malware* simile ad un virus ma che non necessita di legarsi ad altri programmi eseguibili per diffondersi, in quanto utilizza le e-mail o le reti di computer. Solitamente i *worm* danneggiano o distruggono i file dei dispositivi aggrediti;
- **Trojan (**o cavallo di Troia**)** [10]**:** *malware* che assume l'apparenza di *software* legittimo, ma che consente accessi non autorizzati al computer della vittima. I *trojan* vengono utilizzati per rubare dati finanziari o per installare altre minacce e, più in generale per assumere il controllo remoto del terminale all'insaputa del legittimo proprietario[11];

---

[7] Il termine *malware* nasce dalla contrazione di "*malicious software*" (*software* malevolo).

[8] In particolare, i *malware* si attivano nel momento in cui l'utente apre un collegamento o un allegato apparentemente innocuo che, però, installa sul dispositivo uno o più *software* pericolosi.

[9] Si tratta di file di tipo eseguibile es. *.exe, *.bat in grado di integrarsi nei codici eseguibili (incluso il sistema operativo) del sistema informatico vittima, senza essere rilevati dall'utente. Un virus informatico è capace di replicarsi autonomamente, quando vengono eseguiti i programmi infettati e, così, diffondersi nell'intero sistema informatico.

[10] Il nome è ispirato all'Iliade e alla vicenda della guerra di Troia, in quanto il *trojan* si nasconde all'interno di un altro programma apparentemente utile e innocuo. Un *trojan* può contenere qualsiasi tipo di istruzione malevola. Spesso i *trojan* sono usati come veicolo alternativo ai *worm* e ai virus per installare delle *backdoor* o dei *keylogger* sui sistemi bersaglio.

[11] Un particolare tipo di utilizzo dei *trojan*, sempre più diffuso, è rappresentato dal c.d. *cryptomining dannoso* (o *drive-by mining* o *cryptojacking*). Attraverso l'installazione di un *trojan* i criminali informatici sono in grado di utilizzare le risorse del computer infettato per "*estrarre*" criptovalute (*mining*) ed inviare, poi, la valuta raccolta ai propri account.

- **Rootkit**: *malware* che fornisce agli *hacker* l'acceso a dispositivo bersaglio con i privilegi da amministratore. I *rootkit* operano in maniera da rimanere invisibili agli utenti, altri *software* e al sistema operativo stesso[12];
- **Spyware:** *software malevolo* che spia segretamente le attività e i comportamenti dell'utente, al fine di far acquisire ai criminali informatici informazioni utili da sfruttare a proprio vantaggio (es. dati delle carte di credito);
- **Keylogger:** *malware* o dispositivi *hardware* in grado interporsi tra la tastiera e il sistema operativo di computer o altri dispositivi (eventualmente come processo di *background*), in grado di registrare qualsiasi *input* proveniente dalla tastiera, memorizzare le informazioni raccolte e inviarle ai criminali informatici[13]. Di norma i *keylogger* di tipo *software* infettano i PC attraverso un *malware* più grandi, di cui fanno parte;
- **Ransomware:** *malware* che impedisce all'utente l'accesso al proprio dispositivo o ai dati criptando i file. Solitamente il *ransomware* è associato ad una richiesta di un riscatto per poter sbloccare i file criptati;
- **Adware:** *software* indesiderati utilizzati per presentare materiale pubblicitario (spesso all'interno del *browser*) che presentandosi come una componente legittima possono essere utilizzati per diffondere *malware;*
- **Botnet**: rete di dispositivi infettati da *malware* (detti *bot* o *zombie*) che i criminali informatici riescono a controllare tramite un unico dispositivo (detto *botmaster*). Il Botnet permette l'esecuzione di *task online* senza l'autorizzazione dell'utente ed aumenta esponenzialmente le capacità offensive di chi ha sferrato l'attacco. Attraverso i dispositivi infettati è possibile lanciare attacchi definiti *Distributed Denial of Service* (attacco DDoS)[14] contro altri sistemi.

[12] In alcuni casi i *rootkit* possono arrivare ad infettare anche il *firmware* dei dispositivi infettati.
[13]In tal modo i cybercriminali riescono ad ottenere informazioni sensibili come nomi utente, password, PIN delle carte di credito, ecc.
[14] Gli attacchi di tipo *Distributed Denial of Service* (*attacco distribuito di negazione del servizio*) determinano l'esaurimento delle risorse di un sistema informatico che fornisce un servizio *on line* attraverso una crescita esponenziale delle richieste (e, più in generale, del traffico dei dati in entrata) rivolte al sistema bersaglio da molte fonti diverse.

1.2.2 Le altre minacce informatiche

Nel corso del tempo a fianco ai *malware* il crimine informatico ha elaborato anche modalità differenti per utilizzare illegalmente e a proprio vantaggio dati, informazioni e sistemi informatici o per interferire con servizi in rete o attività aziendali. Si tratta di condotte criminali abbastanza sofisticate che interferiscono con le modalità di funzionamento dei sistemi di elaborazione o di comunicazione, insinuandosi nei punti di eventuali debolezza dei sistemi stessi. Tra questi i più diffusi sono:

- **Immissione di codice SQL**: attacco informatico finalizzato al furto dei dati contenuti in un'applicazione *web* interfacciata con un *database* (tipico esempio sono le pagine *web* degli erogatori di servizi *on line* che richiedono un nome utente e una *password*), attraverso l'inserimento nel *database* stesso di un'istruzione SQL dannosa, che permette l'accesso alle informazioni sensibili contenute nel *database*;
- **Attacco *Man-in-the-Middle***: minaccia informatica in cui il criminale informatico, allo scopo di sottrarre dati. intercetta, ritrasmette o altera segretamente le comunicazioni fra due parti che credono di comunicare direttamente tra di loro;
- **Attacco *Denial of Service***: attacchi informatici che mirano ad impedire agli utenti l'accesso alla rete, ad un server *web*, FTP o di posta elettronica attraverso l'invio di molti pacchetti di richieste con la finalità di saturare le risorse e di un dato sistema[15];
- **Attacco MITM**: attacco in cui il criminale informatico si inserisce nel flusso di informazioni che si instaura tra un utente e una rete Wi-Fi pubblica non protetta. Di norma ciò avviene attraverso un *malware* che consente l'acquisizione fraudolenta di informazioni riservate.

1.3 I contenuti della *Cybersecurity*

Le *policy* di sicurezza informatica sono rivolte verso tutti i potenziali rischi provenienti da soggetti sia interni che esterni all'organizzazione ed operativamente agisce su due livelli principali:

- il livello di *sicurezza fisica ed ambientale* che attiene alle componenti *hardware* ed alle condizioni in cui dette componenti operano (ad es. la limitazione dell'accesso fisico nei locali in cui sono custoditi *server* ed altre componenti critiche);

[15] L'elevato numero di richieste rende il sistema *instabile* e non disponibile agli altri utenti. Il sovraccarico di reti e *server* impedisce, infatti, al servizio di soddisfare le richieste legittime;

- livello di *sicurezza logica* che attiene, invece, agli strumenti di tipo *software*.

In ragione dello specifico oggetto di protezione le attività di *cybersecurity* possono essere classificate in diverse categorie:

- **Sicurezza di rete**: insieme di strategie, procedure e tecnologie finalizzate a proteggere le reti informatiche dalle azioni dei criminali informatici (come attacchi mirati o *malware* opportunistici) finalizzate ad accedere a una rete, a modificarla o a violarla[16]. Estremamente importante, in quest'ambito, è la capacità di prevenire ed individuare eventuali intrusioni fornendo risposte adeguate;
- **Sicurezza delle applicazioni**: insieme di strategie, procedure e tecnologie per la protezione dei *software* e dei dispositivi da possibili minacce che potrebbero consentire a soggetti non autorizzati l'accesso i dati e informazioni meritevoli di protezione o permettere di apportare modifiche al codice dall'applicazione[17]. Per garantire la sicurezza delle applicazioni si utilizzano *hardware*, *software* e procedure specifici che mirano ad identificare e minimizzare i fattori di vulnerabilità
- **Sicurezza delle informazioni**: insieme di strategie, procedure e tecnologie per la protezione del patrimonio informativo di una organizzazione (tra cui rientrano anche i dati detenuti a titolo temporaneo) da accessi, divulgazioni, utilizzi, alterazioni, interruzioni o distruzioni non autorizzate, al fine di garantire integrità[18], riservatezza[19] e disponibilità[20]. La sicurezza delle informazioni copre un campo più ampio della cybersicurezza e si concentra principalmente sulla prevenzione di fughe, distorsioni e distruzione di informazioni;
- **Sicurezza operativa**: gestione e protezione degli asset di dati attraverso attente *policy* in tema di autorizzazioni utilizzate dagli utenti per accedere ad una rete e di procedure standardizzate per la memorizzazione o la condivisione dei dati;

[16] La sicurezza di rete si raggiunge integrando più linee di difesa in corrispondenza delle possibili criticità. In primo luogo è necessaria un'adeguata *policy* di controllo degli accessi alla rete che riguardi sia gli utenti autorizzati, sia i dispositivi collegati e i dati immessi. Un'altra linea di difesa di particolare importanza è rappresentata dalla capacità di filtrare, grazie ad appositi dispositivi *hardware* o *software*, denominati *firewall*, il traffico in entrata e in uscire dalla rete.

[17] Per poter massimizzare l'efficacia delle strategie di sicurezza delle applicazioni è necessario che la sua implementazione venga programmata già nella fase di progettazione dell'applicazione stessa.

[18] Dati ed informazioni devono essere protetti rispetto ad interventi ed alterazioni illeciti che ne compromettono validità, accuratezza o completezza.

[19] L'accesso alle informazioni deve essere consentito solo agli utenti autorizzati. A tal fine è necessario proteggerle da accessi non autorizzati da parte di soggetti interni ed esterni all'organizzazione.

[20] I soggetti autorizzati devono poter disporre dei dati nel momento stesso in cui ne hanno bisogno, secondo i requisiti di servizio stabiliti. Occorre, quindi, che le informazioni siano protette da eventi che possano comprometterne la disponibilità (guasti, interruzioni delle connessioni di rete, ecc.).

- ***Disaster recovery* e continuità operativa**: strategie che permettono di rispondere efficacemente a qualsiasi evento che determina una perdita in termini di operazioni o dati (inclusi gli incidenti di *cybersecurity*)[21];
- **Formazione degli utenti finali**: adeguamento della capacità e della propensione degli utenti al rispetto delle procedure di sicurezza per minimizzare il rischio di introdurre accidentalmente un *malware* o altre minacce in un sistema altrimenti sicuro (es. eliminare e-mail sospette, non inserire unità USB di cui non se ne conosce il grado di sicurezza, ecc.).

1.4. La *Cybersecurity* e le attività dinamiche connesse

Considerando in chiave approfondita il macro-tema della Cybersecurity appare necessaria una valutazione di carattere interdisciplinare. In prima istanza appare opportuno considerare **l'analisi euristica**. Nel merito si tratta di un metodo di rilevazione dei virus basato sull'esame del codice informatico per la ricerca di proprietà sospette, segmenti infetti o dubbi, anomalie e comandi pericolosi[22].

Tale modalità di analisi consente anche di intercettare facilmente le anomalie e permette di prevenire la comparsa di virus, ostacolando la proliferazione di nuove minacce in una novazione costante e progressiva[23]. Dal punto di vista pratico l'analisi euristica consente di poter aumentare il livello di sicurezza informatica raffinando gli strumenti di difesa contro ogni tipo di *cyber attacco*. Proprio per tali ragioni l'analisi euristica rappresenta una delle tecniche di base per lo sviluppo dei *software* antivirus[24] Queste caratteristiche sono interconnesse con l'economicità e il costante aggiornamento operato dagli sviluppatori, dai programmatori e dai produttori di antivirus.

Ulteriore elemento dinamico che afferisce al macro-ambito Cybersecurity è il *pattern recognition* che declina specialisticamente l'area dell'apprendimento automatico.

---

[21] La *disaster recovery* individua le procedure utili per ripristinare le operazioni e le informazioni di un'organizzazione e, conseguentemente, la capacità operativa disponibile prima dell'evento. La *continuità operativa* sta ad indicare la capacità di un'organizzazione di mantenere determinati standard nell'erogazione di prodotti e servizi successivamente al verificarsi di un incidente.

[22] I metodi tradizionali di rilevamento dei virus sono, per lo più, basati sul confronto del codice di un programma con quello di virus già noti e registrati in un *database* (il c.d. *rilevamento delle firme*). Tale metodologia, però, nel tempo si è rivelata, almeno in parte, non adeguata di fronte allo sviluppo delle nuove minacce. L'approccio euristico permette, invece, di superare i limiti in questione in quanto è in grado di offrire una difesa più efficace.

[23] L'analisi euristica, infatti, permette di combattere anche i virus c.d. *polimorfici*, ossia quelli il cui codice dannoso è in grado di cambiare e adattarsi costantemente.

[24] Diventa, quindi strategica la capacità di fornire una rapidissima identificazione di virus e programmi indesiderati e la connessa dinamicità di esecuzione. In tale ultima prospettiva, cruciale per la sicurezza informatica, tale forma di analisi assume centralità costruendo nel tempo una memoria strutturata inerente il comportamento dei *malware***.** In questo modo si dà vita a numerosi database in cui sono presenti tutte le informazioni relative a intere famiglie di *malware*.

Specificamente, la *pattern recognition* è una tecnologia che consente alle macchine di rilevare disposizioni di caratteristiche o dati che forniscono alcune informazioni importanti su un dato sistema[25]. Si tratta, quindi, di una *dinamica di sicurezza informatica attiva* che si radica nel processo di osservazione ed elaborazione i dati, volto all'identificazione di eventuali regolarità all'interno dei dati stessi. I *pattern* da classificare sono tipicamente gruppi di misure che definiscono punti in uno spazio multidimensionale (al contrario del *pattern matching*, in cui il pattern è specificato in modo rigido). Da molti anni i motori di analisi euristica e di riconoscimento dei *pattern* d'azione dei sistemi operano con tali tecnologie per aumentare la protezione e fornire una difesa innovativa in grado di adattarsi alle tante minacce che animano il mondo del web e quello informatico in generaleIn una visione interdisciplinare la cybersicurezza si connette con l'**intelligenza artificiale** cioè con l'insieme di tecnologie che combinano dati, algoritmi e potenze di calcolo.

L'impatto dei sistemi di intelligenza artificiale può essere considerato non solo da una prospettiva individuale del cittadino, ma anche dal punto di vista della società nel suo complesso in relazione al suo impatto su pubbliche amministrazioni e imprese

1.5 La moderna gestione delle minacce

Come si è già avuto modo di sottolineare, i sistemi informativi delle moderne organizzazioni (pubbliche amministrazioni, aziende, ecc.) si caratterizzano per un elevato grado di complessità che se da un lato permette il trattamento di una ingente mole di dati e l'erogazione di servizi capillari ed articolati, dall'altro espone tali sistemi informativi a rischi specifici quali *malware* mutevoli[26], APT (*Advanced Persistent Threats* - Minacce avanzate persistenti[27]),

[25] Per comprendere tale concetto è necessario riflettere sull'analisi computazionale delle immagini e dei modelli più astratti. Nel dettaglio, la tecnologia di *computer vision* comporta l'acquisizione di immagini digitali utilizzando sensori di immagine, l'elaborazione e l'analisi delle foto per acquisire una certa comprensione dell'*input* visivo. La *visione artificiale* è un sottoinsieme dell'*intelligenza artificiale* ed è utilizzata per estrarre informazioni significative dalle immagini. La *computer vision* è un campo dell'apprendimento automatico e dell'intelligenza artificiale che si occupa di come i *computer* possono essere addestrati a ricavare informazioni significative da immagini o video digitali. Viene utilizzata in un'ampia gamma di aree applicative, come il riconoscimento facciale, il rilevamento dei difetti, la verifica dell'assemblaggio, il rilevamento degli intrusi e sicurezza dei *server*. Per l'interpretazione delle minacce potenziali e attuali ai sistemi informatici, la *computer vision* è strettamente correlata alla *pattern recognition*. Il riconoscimento dei modelli o riconoscimento degli schemi è un metodo di analisi dei dati che riconosce modelli e regolarità dei flussi informatici utilizzando algoritmi di apprendimento automatico. È uno studio su come le macchine possono classificare gli oggetti in una serie di categorie e classi similmente a come il cervello umano valuta il gli accadimenti esterni.

[27] La locuzione anglosassone *Advanced Persistent Threat* (in italiano *minaccia avanzata e persistente*), individua una minaccia informatica posta in essere da criminali informatici dotati di elevate competenze tecniche e grandi risorse umane e finanziarie e, quindi, in grado di realizzare attacchi su larga scala, non visibili, protratti per lunghi periodi di tempo. Le APT sono finalizzate ad ottenere informazioni riservate o a rendere inutilizzabili alcuni servizi dell'organizzazione attaccata per motivazioni generalmente politiche o economiche. Gli attacchi APT sono molto utilizzati anche per il cyberspionaggio.

minacce interne[28]. Ulteriori momenti di vulnerabilità possono essere legati all'utilizzo di soluzioni *cloud* per il trattamento dei dati e l'erogazione dei servizi e per l'impiego della forza lavoro (tutto o in parte) *remota*[29].

I più comuni sistemi di gestione delle minacce seguono un'architettura logica di supporto riferita a standard internazionali comuni[30] che individuano cinque funzioni fondamentali:

- ***Identificazione***: individuazione dettagliata degli asset e delle risorse più importanti dell'organizzazione quali la gestione delle risorse, la *mission* istituzionale, la *governance*, la valutazione dei rischi, la strategia di gestione dei rischi;
- ***Protezione***: messa in atto delle verifiche e dei controlli di sicurezza tecnica e fisica finalizzati allo sviluppo e all'implementazione di livelli di sicurezza efficace e alla protezione di infrastrutture critiche[31].;
- ***Rilevamento***: perfezionamento di misure in grado di segnalare all'organizzazione i possibili attacchi informatici. L'attività di rilevamento comprende: la segnalazione delle anomalie e degli eventi critici, il monitoraggio continuo della sicurezza e l'implementazione dei processi di rilevamento precoce;
- ***Risposta***: reazione appropriata agli attacchi informatici e ad altri eventi di sicurezza informatica. Questa fase comporta la pianificazione della risposta, la comunicazione, l'analisi, la mitigazione del danno e i miglioramenti del sistema di gestione delle minacce;
- ***Ripristino***: Implementazione dei piani per la resilienza informatica al fine di garantire la continuità operativa in caso di attacco informatico, violazione della sicurezza o altri eventi di sicurezza informatica.

[28] Le minacce interne sono rappresentate da un uso improprio dei dati di un'organizzazione (pubbliche amministrazioni, aziende, ecc.) per cause accidentali o dolose. Le minacce interne sono particolarmente pericolose per la sicurezza informatica di PA e imprese e possono rivelarsi più costose delle minacce esterne.
[29] Di norma i dispositivi utilizzati dai *lavoratori remoti* sono meno protetti rispetto alle reti interne di PA e imprese, e rappresentano, quindi, uno degli anelli deboli della catena di protezione dalle aggressioni esterne. Occorre, infatti, tener presente che rispetto a tali aggressioni la protezione offerta dai normali *software* antivirus risulta, per lo più, insufficiente.
[30] Nello specifico il riferimento è al *framework* di sicurezza informatica istituito dal *National Institute of Standards and Technology* (NIST) definito nella guida denominata *NIST Cybersecurity Framework* (NIST CF) ove, anche con il ricorso a standard e *best practice*, il NIST fornisce una guida completa per migliorare la sicurezza delle informazioni e la gestione dei rischi relativi alla sicurezza informatica per le organizzazioni del settore privato.
[31] Rientrano in quest'ambito la gestione delle identità, il controllo degli accessi, la formazione, la sicurezza dei dati, i processi e le procedure di sicurezza delle informazioni, la manutenzione e la tecnologia di protezione.

Capitolo II: La Cybersicurezza nella normativa italiana: il DECRETO-LEGGE 14 giugno 2021, n. 82

2.1 L'architettura istituzionale

Con il D.L. 14 giugno 2021, n. 82, *Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale* – convertito con modificazioni dalla L. 4 agosto 2021, n. 109 – il legislatore è intervenuto con un primo, significativo provvedimento di attuazione dei principi espressi dal PNRR in tema di *cybersicurezza*.
Tale normativa ha rimodellato l'architettura istituzionale di cybersicurezza, riorganizzando quadro normativo di riferimento, ruoli e responsabilità specifiche delineando, così, una nuova cornice di *governance* istituzionale, incardinata su di una nuova agenzia pubblica specializzata – denominata *Agenzia per la cybersicurezza nazionale* – vocata alla costruzione e allo sviluppo di capacità nazionali di resilienza cibernetica. Tale normativa ha rimodellato l'architettura istituzionale di cybersicurezza, riorganizzando quadro normativo di riferimento, ruoli e responsabilità specifiche delineando, così, una nuova cornice di governance istituzionale, incardinata su di una nuova agenzia pubblica specializzata – denominata Agenzia per la cybersicurezza nazionale – vocata alla costruzione e allo sviluppo di capacità nazionali di resilienza cibernetica.

La cruciale tematica della gestione della sicurezza cibernetica sul piano sistemico, costituisce uno snodo fondamentale per gli interventi del *Piano Nazionale di Ripresa e Resilienza* (c.d. "PNRR"), trasmesso dal Governo alla Commissione europea il 30 aprile 2021, all'interno del primo intervento della missione 1 relativa alla *Digitalizzazione, innovazione, competitività, cultura e turismo*. Nel merito, le linee strategiche del Piano desiderano sostenere la transizione digitale del Paese per offrire a cittadini e imprese servizi efficaci, in sicurezza e pienamente accessibili. In particolare, relativamente agli aspetti di cybersercurity il PNRR si prende cura del rafforzamento dei presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio intercettatati verso la PA e le imprese di interesse nazionale. Inoltre il Piano pone lo sguardo sulla costruzione e il consolidamento delle capacità tecniche di valutazione e audit continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale e sull'irrobustimento degli asset e delle unità cyber incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber. A tale intervento sono destinati investimenti per circa 620 milioni di euro,

distribuiti nel quadriennio 2021-2024, con un impulso determinante nell'attuazione effettiva della nuova *governance* istituzionale e alle funzioni della Agenzia per la cybersicurezza nazionale. Alla luce di tale cornice introduttiva, i temi trattati nei paragrafi successivi analizzano le principali linee, tra loro interconnesse, sottese all'introduzione del D.L. 82/2021 in considerazione della necessità di ridefinire la *governance* istituzionale di cybersicurezza e la connessa necessità di riorganizzare il quadro normativo nazionale applicabile.

La ridefinizione dell'architettura istituzionale di cybersicurezza contenuta nelle norme si sostanzia in una serie di interventi finalizzati a riordinare i diversi ambiti di operatività della cybersicurezza nazionale (ambiti correlati, ma comunque distinti) e propedeutici, da un lato, **allo sviluppo di capacità di resilienza cibernetica nazionale** e, dall'altro lato, **allo svolgimento di attività di "*cyber-intelligence*"** (di competenza degli organismi di informazione per la sicurezza), di ***cyber-defense*** (intesa come difesa e sicurezza militare dello Stato, di competenza del Ministero della difesa) e alla ***prevenzione e repressione dei reati*** (di competenza delle Forze di polizia)[32]. Nel merito, il D.L. n. 82/2021 pone al centro delle politiche di implementazione e sviluppo dei sistemi di sicurezza informatica la Presidenza del Consigli dei Ministri e il ***Comitato interministeriale per la cybersicurezza***. In particolare, l'art. 2 del D.L. n. 82/2021, attribuisce in via esclusiva alla competenza del Presidente del Consiglio dei ministri le seguenti funzioni in materia di *cybersicurezza*:

a) l'alta direzione e la responsabilità generale delle politiche di *cybersicurezza*;
b) l'adozione della strategia nazionale di *cybersicurezza*, sentito il *Comitato interministeriale per la cybersicurezza* ;
c) la nomina e la revoca del direttore generale e del vice direttore generale dell'*Agenzia per la cybersicurezza nazionale*, previa deliberazione del Consiglio dei ministri.

Ai fini dell'esercizio delle competenze relative all'alta direzione delle politiche di *cybersicurezza*, il Presidente del Consiglio dei ministri, sentito il Comitato, impartisce le relative direttive ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'*Agenzia per la cybersicurezza nazionale*.

Il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può demandare le funzioni che lo stesso D.L. 82/2021 gli attribuisce in via non esclusiva all'*Autorità delegata* di cui all'art. 3, della L. 3 agosto 2007, n. 124[33]. In tal caso il Presidente del Consiglio dei ministri resta

[32] Rivista Privacy& n. 3 ottobre 2021

[33] Il primo comma del citato art. 3 della L. n. 124/2007, prevede che il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare le funzioni che non sono ad esso attribuite in via esclusiva soltanto ad un *Ministro senza portafoglio* o ad un *Sottosegretario di Stato*, denominati "*Autorità delegata*". L'*Autorità delegata* non può esercitare funzioni di governo ulteriori rispetto a quelle ad essa delegate, ad eccezione delle funzioni attribuite al Sottosegretario di Stato alla Presidenza del Consiglio dei ministri, con funzioni di Segretario del Consiglio medesimo.

costantemente informato dall'*Autorità delegata* circa le modalità di esercizio delle funzioni delegate e, fermo restando il potere di direttiva, può in qualsiasi momento avocare l'esercizio di tutte o di alcune di esse.

L'Autorità delegata, in relazione alle funzioni delegate in materia di *cybersicurezza*, partecipa alle riunioni del *Comitato interministeriale per la transizione digitale*.

– Il Comitato interministeriale per la cybersicurezza

Presso la Presidenza del Consiglio dei ministri è istituito, ai sensi dell'art. 4 del D.L. n. 82/2021, il *Comitato interministeriale per la cybersicurezza* (CIC), con funzioni di *consulenza*, *proposta* e *vigilanza* in materia di politiche di *cybersicurezza*. Il CIC è presieduto dal *Presidente del Consiglio dei ministri* ed è composto dall'*Autorità delegata per la sicurezza della Repubblica*, dal *Ministro degli affari esteri e della cooperazione internazionale*, dal *Ministro dell'interno*, dal *Ministro della giustizia*, dal *Ministro della difesa*, dal *Ministro dell'economia e delle finanze*, dal *Ministro delle imprese e del made in Italy*, dal *Ministro dell'ambiente e della sicurezza energetica*, dal *Ministro dell'università e della ricerca* e dal *Ministro delle infrastrutture e dei trasporti*. Le funzioni di segretario del CIC sono svolte dal Direttore Generale dell'Agenzia.

Il Presidente del Consiglio dei ministri, inoltre, può invitare alle sedute del Comitato, anche a seguito di loro richiesta e senza diritto di voto, altri componenti del Consiglio dei ministri, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare.

In particolare, il Comitato:

a) propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di *cybersicurezza* nazionale;
b) esercita l'*alta sorveglianza* sull'attuazione della strategia nazionale di *cybersicurezza*;
c) promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla *cybersicurezza*, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della *cybersicurezza* e allo sviluppo industriale, tecnologico e scientifico in materia di *cybersicurezza*;
d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la *cybersicurezza* nazionale.

Il sesto comma dell'art. 4 chiarisce che il Comitato svolge altresì le funzioni già attribuite al *Comitato interministeriale per la sicurezza della Repubblica* (CISR), dal c.d. *decreto-legge*

perimetro[34] e dai relativi provvedimenti attuativi (fatta eccezione per le determinazioni del Presidente del Consiglio dei ministri previste dall'art. 5 dello stesso decreto-legge perimetro in caso di crisi di natura cibernetica).

– L'Agenzia per la cybersicurezza nazionale

L'art. 5 del D.L. n. 82/2021 istituisce, a tutela degli interessi nazionali nel campo della *cybersicurezza*, l'*Agenzia per la cybersicurezza nazionale*, con sede in Roma.

L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti previsti dalla legge. Il Presidente del Consiglio dei ministri e l'Autorità delegata (ove istituita) si avvalgono dell'Agenzia per l'esercizio delle competenze indicate dal D.L. n. 82/2021.

Il direttore generale ha la rappresentanza legale dell'Agenzia. Egli è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata (ove istituita), ed è gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia.

Il direttore generale dell'Agenzia è scelto tra magistrati delle giurisdizioni superiori ordinaria ed amministrativa, avvocati dello Stato, dirigenti generali dello Stato ed equiparati, professori universitari di ruolo ovvero tra estranei alla pubblica amministrazione in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione.

Gli incarichi del direttore generale e del vice direttore generale hanno la durata massima di quattro anni e sono rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni[35].

L'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di precipua competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle Forze armate, delle forze di polizia o di enti pubblici per lo svolgimento dei suoi compiti istituzionali[36].

[34] L'art. 1, comma 1, lett. c) del D.L n. 82/2021 con la locuzione *decreto perimetro* indica il D.L. 21 settembre 2019, n. 105 (convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*), recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*.

[35] Il direttore generale ed il vice direttore generale, ove provenienti da pubbliche amministrazioni sono collocati fuori ruolo o in posizione di comando o altra analoga posizione, secondo gli ordinamenti di appartenenza.

[36] Inoltre, ai sensi di quanto previsto dall'articolo 31, comma 3, della legge 3 agosto 2007, n. 124, il COPASIR, può chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza.

2.2 L'Organizzazione dell'Agenzia per la cybersicurezza nazionale

L'organizzazione, l'articolazione e il funzionamento dell'Agenzia sono definiti da un apposito regolamento adottato con decreto del Presidente del Consiglio dei ministri[37], entro centoventi giorni dalla data di entrata in vigore della legge di conversione del D.L. 82/2021[38].
Sono organi dell'Agenzia:

- il Direttore Generale;
- il Collegio dei revisori dei conti.

Con il regolamento sull'organizzazione e il funzionamento dell'agenzia sono disciplinati altresì:

a) le funzioni del Direttore generale e del Vice direttore generale dell'Agenzia;
b) la composizione e il funzionamento del Collegio dei revisori dei conti;
c) l'istituzione di eventuali sedi secondarie.

2.3 Le Funzioni dell'Agenzia per la cybersicurezza nazionale

L'Agenzia, ai sensi dell'art. 7del D.L. n. 82/2021:

a) è *Autorità nazionale per la cybersicurezza* e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni[39], il coordinamento tra i soggetti pubblici coinvolti in materia di *cybersicurezza* a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore;
b) predispone la strategia nazionale di *cybersicurezza*;
c) svolge ogni necessaria attività di supporto al funzionamento del *Nucleo per la cybersicurezza*;

[37] Di concerto con il Ministro dell'economia e delle finanze, anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, previo parere delle Commissioni parlamentari competenti per materia e per i profili finanziari e, per i profili di competenza, del COPASIR, sentito il *Comitato interministeriale per la cybersicurezza* CIC.
[38] In particolare l'Agenzia può essere articolata fino ad un numero massimo di otto uffici di livello dirigenziale generale, nonché fino ad un numero massimo di trenta articolazioni di livello dirigenziale non generale nell'ambito delle risorse finanziarie destinate all'Agenzia.
[39] In particolare, restano ferme le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge 1° aprile 1981, n. 121 *Nuovo ordinamento dell'Amministrazione della pubblica sicurezza*.

d) è Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS[40], a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto;
e) è Autorità nazionale di certificazione della cybersicurezza e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al *Ministero dello sviluppo economico* dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni;
f) assume tutte le funzioni in materia di *cybersicurezza* già attribuite dalle disposizioni vigenti al *Ministero dello sviluppo economico*, ivi comprese quelle relative al perimetro di sicurezza nazionale cibernetica, alla sicurezza e all'integrità delle comunicazioni elettroniche e alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;
g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento (istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56);
h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi;
i) assume tutte le funzioni già attribuite al *Dipartimento delle informazioni per la sicurezza* (DIS)
l) provvede, sulla base delle attività di competenza del *Nucleo per la cybersicurezza* alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro per le ipotesi di crisi di natura cibernetica;
m) assume tutte le funzioni in materia di *cybersicurezza* già attribuite all'*Agenzia per l'Italia digitale* dagli artt. 51 e 71[41] del CAD. L'Agenzia assume, altresì, i compiti di determinare, con proprio regolamento i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione e di definizionedelle caratteristiche di qualità, sicurezza, *performance* e scalabilità, interoperabilità, portabilità dei servizi *cloud* per la pubblica

[40] L'art. 1, comma 1, lett. d) del D.L. n. 82/2021 per *decreto legislativo NIS* intende il D.Lgs. 18 maggio 2018, n. 65, di attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
[41] Con particolare riferimento al potere di adottare linee guida contenenti regole tecniche di *cybersicurezza* ai sensi dell'articolo 71 del CAD.

amministrazione (di cui all'art. 33-*septies*, comma 4, del D.L. 18 ottobre 2012, n. 179, già attribuiti all'Agenzia per l'Italia digitale);

m-*bis*) assume le iniziative idonee a valorizzare la crittografia come strumento di *cybersicurezza*, anche attraverso un'apposita sezione dedicata nell'ambito della strategia nazionale di *cybersicurezza*. In particolare, l'Agenzia attiva ogni iniziativa utile volta al rafforzamento dell'autonomia industriale e tecnologica dell'Italia, valorizzando lo sviluppo di algoritmi proprietari nonché la ricerca e il conseguimento di nuove capacità crittografiche nazionali;

m-*ter*) provvede alla qualificazione dei servizi *cloud* per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea;

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità;

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

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

q) coordina, in raccordo con il *Ministero degli affari esteri e della cooperazione internazionale*, la cooperazione internazionale nella materia della *cybersicurezza*[42];

r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di *cybersicurezza* e, in particolare, con il *Ministero della difesa* per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati

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

dello sviluppo della *cybersicurezza*, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo;

s) stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di *cybersicurezza*, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di *cybersicurezza*, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della *cybersicurezza* e dei correlati servizi applicativi, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

u) svolge attività di comunicazione e promozione della consapevolezza in materia di *cybersicurezza*, al fine di contribuire allo sviluppo di una cultura nazionale in materia;

v) promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della *cybersicurezza*, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;

v-bis) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni[43];

z) per il perseguimento delle proprie finalità istituzionali, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri;

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

[43] In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile.

Presso l'Agenzia, anche ai fini dell'esercizio delle funzioni sub r), s), t), u), v), z) e aa), è istituito, con funzioni di consulenza e di proposta, un *Comitato tecnico-scientifico*, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri[44]. La composizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento che disciplina l'organizzazione, l'articolazione e il funzionamento dell'Agenzia.

Il CSIRT (Computer Security Incident Response Team) italiano, che svolge i compiti e le funzioni del *Computer Emergency Response Team* (CERT) nazionale è trasferito presso l'Agenzia e assume la denominazione di: «*CSIRT Italia*».

È trasferito, altresì presso l'Agenzia anche il Centro di valutazione e certificazione nazionale.

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

– Il Nucleo per la cybersicurezza

L'art. 8 del D.L. n. 82/2021 costituisce in via permanente, presso l'Agenzia, il *Nucleo per la cybersicurezza*, a supporto del Presidente del Consiglio dei ministri nella materia della *cybersicurezza*, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. Il Nucleo per la cybersicurezza è presieduto dal *Direttore Generale dell'Agenzia* o, per sua delega, dal *Vice Direttore Generale*, ed è composto *dal Consigliere militare del Presidente del Consiglio dei ministri*, da un rappresentante, rispettivamente, del *Dipartimento delle informazioni per la sicurezza* (DIS), dell'*Agenzia informazioni e sicurezza esterna* (AISE), dell'*Agenzia informazioni e sicurezza interna* (AISI), del *Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri* (PCM), del *Ministero degli esteri e della cooperazione internazionale* (MAECI), del *Ministero dell'interno*, del *Ministero della giustizia*, del *Ministero della difesa*, del *Ministero dell'economia e delle finanze* (MEF), del *Ministero delle imprese e del made in Italy* (MIMIT), del *Ministero dell'ambiente e della sicurezza energetica* (MASE), del *Ministero dell'università e della ricerca* (MUR), del *Ministero delle infrastrutture e dei trasporti* (MIT)

[44] Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.

e del *Dipartimento della protezione civile* della PCM. Per gli aspetti relativi alla trattazione di informazioni classificate[45] il Nucleo è integrato da un rappresentante dell'*Ufficio centrale per la segretezza*. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza. Il Nucleo può essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi. In situazioni di crisi di natura cibernetica il Nucleo è integrato, in ragione della necessità, con un rappresentante, rispettivamente, del *Ministero della salute* e del *Ministero dell'interno-Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile*.

2.3.1 Tavolo interministeriale Perimetro di Sicurezza Nazionale Cibernetica

Ai sensi dell'art. 10 del D.L. 82/2021, qualora nella gestione di situazioni di crisi che coinvolgono aspetti di *cybersicurezza*, il Presidente del Consiglio dei ministri convochi il CISR alle sedute di quest'ultimo sono chiamati a partecipare il (ministro) *delegato per l'innovazione tecnologica e la transizione digitale* e il *Direttore generale dell'Agenzia*. Il *Perimetro di Sicurezza Nazionale Cibernetica* è stato istituito dal D.L. n. 105 del 2019 al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Per assicurare il raccordo tra le amministrazioni impegnate, a vario titolo, nell'attuazione del *Perimetro di Sicurezza Nazionale Cibernetica* è istituito, presso l'Agenzia per la cybersicurezza nazionale e presieduto dal proprio Direttore Generale, il *Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica* (articolo 6 del decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131), cosiddetto Tavolo Perimetro, a supporto del CIC, specie in relazione all'individuazione delle funzioni e dei servizi essenziali dello Stato, nonché dei soggetti che li erogano da includere nel Perimetro.

[45] Si tratta delle informazioni inserite nelle classifiche di segretezza di cui all'art. 42, della L. 3 agosto 2007, n. 124. In particolare, le classifiche di segretezza sono attribuite per circoscrivere la conoscenza di informazioni, documenti, atti, attività o cose ai soli soggetti che abbiano necessità di accedervi in ragione delle proprie funzioni istituzionali. La classifica di segretezza è apposta, e può essere elevata, dall'autorità che forma il documento, l'atto o acquisisce per prima la notizia, ovvero è responsabile della cosa, o acquisisce dall'estero documenti, atti, notizie o cose. Le classifiche attribuibili sono: *segretissimo*, *segreto*, *riservatissimo*, *riservato*. Le classifiche sono attribuite sulla base dei criteri ordinariamente seguiti nelle relazioni internazionali.

2.4 Il Trattamento dei dati personali

L'art. 13 del D.L. n. 82/2021 precisa che il trattamento dei dati personali svolto per finalità di sicurezza nazionale in applicazione dello stesso D.L. n. 82/2021 è effettuato ai sensi dell'art. 58, commi 2 e 3, del D.Lgs. 30 giugno 2003, n. 196[46] *Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.*

2.5 Le relazioni annuali

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

Entro il 30 giugno di ogni anno, il Presidente del Consiglio dei ministri trasmette al COPASIR una relazione sulle attività svolte nell'anno precedente dall'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del Comitato.

2.6 L'applicazione del D.L. n. 82/2021

Per lo svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, l'Agenzia ***può provvedere***, oltre che con proprio personale, con l'ausilio dell'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (di cui all'art. 7-*bis* del D.L. 27 luglio 2005, n. 144).

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

---

[46] Nello specifico le norme citate prevedono che:
[…]
2. Fermo restando quanto previsto dal comma 1, ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base a disposizioni di legge o di regolamento o previste da atti amministrativi generali, che prevedano specificamente il trattamento, si applicano le disposizioni di cui al comma 1 del presente articolo, nonché quelle di cui agli articoli 23 e 24 del decreto legislativo 18 maggio 2018, n. 51.
3. Con uno o più regolamenti sono individuate le modalità di applicazione delle disposizioni di cui ai commi 1 e 2, in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies, anche in relazione all'aggiornamento e alla conservazione. I regolamenti, negli ambiti di cui al comma 1, sono adottati ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, e, negli ambiti di cui al comma 2, sono adottati con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su proposta dei Ministri competenti.
[…]

cui al citato art.7-bis del D.L. n. 144/2005). Il personale dell'Agenzia, nello svolgimento delle funzioni ispettive, di accertamento delle violazioni e di irrogazione delle sanzioni, nonché delle funzioni relative all'attuazione e al controllo dell'esecuzione dei provvedimenti assunti da parte del Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del c.d. *decreto-legge perimetro*, riveste la qualifica di pubblico ufficiale.

Riveste, altresì la qualifica di pubblico ufficiale il personale dell'Agenzia addetto al CSIRT Italia, nello svolgimento delle proprie funzioni. La trasmissione delle notifiche di incidente ricevute dal CSIRT Italia all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione costituisce adempimento dell'obbligo di cui all'articolo 331 del codice di procedura penale[47].

Con uno o più decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, da adottare entro centottanta giorni dalla data di entrata in vigore della legge di conversione del D.L. 82/2021, sono definiti i termini e le modalità:

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

In relazione al trasferimento delle funzioni precedentemente di pertinenza dell'AgID detti decreti definiscono, altresì, i raccordi tra le due amministrazioni, per le funzioni che restano di competenza dell'AgID.

L'Agenzia si avvale del patrocinio dell'Avvocatura dello Stato, ai sensi dell'articolo 1 del Testo Unico approvato con R.D. 30 ottobre 1933, n. 1611.

---

[47] L'art. 331 c.p.c. disciplina la *Denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio*:
1. Salvo quanto stabilito dall'articolo 347, i pubblici ufficiali e gli incaricati di un pubblico servizio che, nell'esercizio o a causa delle loro funzioni o del loro servizio, hanno notizia di un reato perseguibile di ufficio, devono farne denuncia per iscritto, anche quando non sia individuata la persona alla quale il reato è attribuito.
2. La denuncia è presentata o trasmessa senza ritardo al pubblico ministero o a un ufficiale di polizia giudiziaria.
3. Quando più persone sono obbligate alla denuncia per il medesimo fatto, esse possono anche redigere e sottoscrivere un unico atto.
4. Se, nel corso di un procedimento civile o amministrativo, emerge un fatto nel quale si può configurare un reato perseguibile di ufficio, l'autorità che procede redige e trasmette senza ritardo la denuncia al pubblico ministero.

Capitolo III: Il Piano nazionale ripresa e resilienza (PNRR) e la Cybersicurezza

3.1 Sicurezza e la Missione 1 del PNRR

La sicurezza delle reti e dei sistemi informatici costituisce uno dei 7 investimenti previsti dal *Piano nazionale di ripresa e resilienza* (PNRR) nell'ambito delle azioni di *Digitalizzazione della pubblica amministrazione*.

La componente 1 della prima Missione 1 del PNRR (*Digitalizzazione, Innovazione e Sicurezza nella PA*)[48] si propone di sviluppare un'offerta integrata e armonizzata di servizi digitali all'avanguardia orientati a cittadini, residenti e imprese. Il raggiungimento di un tale risultato permetterebbe all'Italia di raggiungere gli ambiziosi traguardi fissati in sede europea dal *Digital Compass 2030*, il quale prevede che entro il 2030 tutti i servizi pubblici chiave siano disponibili *online*[49].

Nella prospettiva italiana del PNRR, per il comparto della pubblica amministrazione, lo snodo decisivo è rappresentato dal passaggio al digitale, con particolare riferimento allo sviluppo di servizi *on-line*[50]. In tale sguardo è possibile individuare le infrastrutture realizzate su cui poggia l'intervento programmato nella componente in analisi:

a) l'identità digitale[51];
b) i pagamenti digitali tra cittadini e Pubblica amministrazione[52];
c) le notifiche digitali[53].

Nel dettaglio, il rafforzamento dei servizi pubblici digitali si radica su una serie di interventi *abilitanti*, tra cui la migrazione al *cloud* delle pubbliche amministrazioni, la diffusione della

[48] Alla quale sono destinati circa 9,72 miliardi di euro a cui si somma 1,40 miliardi del *Fondo complementare* di cui al D.L. 6 maggio 2021, n. 59, convertito con modificazioni dalla L. 1° luglio 2021, n. 101.

[49] La *missione 1, componente 1, del PNRR,* si pone in linea di coerenza con il contesto europeo, in cui i diritti e i principi digitali andranno ad integrare i diritti esistenti (come ad es. quelli sanciti dalla *Carta dei diritti fondamentali dell'UE* e dalla legislazione in materia di protezione dei dati e di *privacy*). In tale ambito si completeranno sia il quadro di riferimento per i cittadini sui loro diritti digitali, sia gli orientamenti per gli Stati membri dell'UE e per le imprese che si occupano di nuove tecnologie. Le persone e i loro diritti saranno al centro della trasformazione digitale, grazie ad un processo che:

- sostiene la solidarietà e l'inclusione;
- garantisce la libertà di scelta *online*;
- promuove la partecipazione allo spazio pubblico digitale;
- incrementa la sicurezza, la protezione e la responsabilizzazione delle persone;
- promuove, altresì, la sostenibilità del futuro digitale.

[50] Come quelli appena avviati dall'anagrafe nazionale della popolazione residente e nella migrazione su *cloud pubblico* che rappresenta uno degli investimenti più importanti nell'agenda del sistema paese

[51] Gli obiettivi fissati sono il superamento della soglia di 40 milioni di utilizzatori delle piattaforme esistenti per l'identificazione informatica (CIE e SPID) e la presenza di tutti i comuni nell'*Anagrafe della Popolazione residente* ANPR.

[52] Promuovendo l'adozione di PagoPA in oltre 14.000 amministrazioni locali.

[53] Tramite la creazione della nuova *Piattaforma unica di notifiche digitali* per comunicare efficacemente con cittadini e imprese, garantendo la validità legale degli atti.

App "IO" come punto di accesso preferenziale per il cittadino e il *rafforzamento della cybersecurity nazionale*.

Proprio per ovviare alla necessità di un rafforzamento del generale grado di sicurezza informatica a livello nazionale l'Investimento 1.5 della Missione 1, Componente 1.1, del PNRR (denominato *cybersecurity*) promuove l'implementazione e il potenziamento dei sistemi nazionali di *Cybersecurity*. Specificamente, il *Piano* segnala una serie di criticità che necessitano di un'attenta valutazione del rischio presente e futuro e, quindi, di una risposta adeguata da parte del Paese:

- la sempre maggiore diffusione della digitalizzazione in ogni campo del vivere civile incrementa, su tutti i fronti, il grado complessivo di vulnerabilità della società nei confronti di minacce di tipo cyber (ad es. frodi, ricatti informatici, attacchi terroristici, ecc.)[54].
- la crescente dipendenza da servizi *software* di terze parti comporta una sempre maggiore esposizione dei sistemi delle amministrazioni pubbliche alle *intenzioni* dei fornitori/sviluppatori/proprietari dei servizi stessi;
- l'aumento di interdipendenza tra le diverse PA, aziende controllate dallo Stato, privati)[55].

Il Piano, al fine di favorire una transizione digitale nazionale resiliente, prevede investimenti incentrati sulla capacità di *monitoraggio*, *prevenzione* e *risposta* più efficaci contro le minacce cyber[56] e sulla certificazione delle tecnologie *cyber*. Gli investimenti sono organizzati su quattro aree di intervento principali:

- sono rafforzati i presidi di *front-line* per la gestione degli *alert* e degli eventi a rischio intercettatati verso la PA e le imprese di interesse nazionale;
- sono costruite o rese più solide le capacità tecniche di valutazione e audit continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale;
- si investe nell'immissione di nuovo personale sia nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e investigazione del crimine informatico

54 A tal proposito si evidenzia che la minaccia cibernetica cresce continuamente sia in quantità che in qualità. Tale tendenza è determinata anche dall'evoluzione delle tecniche di ingegneria sociale volte a ingannare gli utenti finali dei servizi digitali.

55 Sotto tale profilo mette conto segnale come, nel corso del tempo si sia assistito ad un incremento notevole degli attacchi rivolti alle *supply chain*, ovvero alle catene dei fornitori di beni e servizi nell'indotto della PA.

56 Per identificare tempestivamente gli eventi informatici malevoli e mitigarne gli effetti dannosi, così da garantire la conservazione e la gestione, in tutta sicurezza, di dati e servizi della Pubblica Amministrazione.

diretto contro singoli cittadini, sia in quelle dei comparti preposti a difendere il paese da minacce cibernetiche;

- sono irrobustiti gli *asset* e le *unità cyber* incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber.

  La realizzazione di tutto ciò si svolge in pieno raccordo con le iniziative Europee finalizzate ad assicurare la protezione degli interessi comuni dei cittadini e delle imprese.[57] Nell'orizzonte del 2024 tali interventi porteranno al dispiego integrale dei *Servizi nazionali di cybersecurity* nonché al completamento della rete dei laboratori a supporto del conseguimento dell'autonomia strategica nazionale nel settore e alla realizzazione di un piano operativo delle attività di monitoraggio tecnico-organizzativo[58].

Il *Piano Nazionale di Ripresa e Resilienza*, l'istituzione della nuova *Agenzia per la Cybersicurezza nazionale* e il decreto attuativo del *Perimetro di sicurezza nazionale cibernetica* pongono la cybersecurity a fondamento della digitalizzazione della Pubblica Amministrazione e del Sistema Italia. In tale contesto sono necessarie infrastrutture tecnologiche e piattaforme in grado di offrire a cittadini e imprese servizi digitali efficaci, sicuri e resilienti.

È necessario, quindi, per tutte le PA un cambio di approccio in cui la *cybersecurity* non può più essere vista come un costo o un mero adempimento normativo, bensì come un'opportunità per la crescita e la trasformazione digitale sia della Pubblica Amministrazione che dell'intero Paese. È questa la chiave di riflessione del PNRR legata alla cybersecurity. Punti focali di questa valutazione sono le tematiche relative al *Cyber Security Awareness*, in quanto da tale consapevolezza possono derivare le azioni organizzative necessarie a mitigare il rischio connesso alle potenziali minacce informatiche e alle evoluzioni degli attacchi informatici[59].

La sicurezza delle reti e dei sistemi informatici deve considerare anche lo sviluppo delle infrastrutture digitali – parte integrante della strategia di modernizzazione del settore pubblico – poiché queste sostengono l'erogazione sia di servizi pubblici a cittadini e imprese sia di servizi essenziali per il Paese. Tali infrastrutture devono essere affidabili, sicure, energeticamente efficienti ed economicamente sostenibili. L'obiettivo di garantire una maggiore efficienza dei sistemi non può essere, infatti, disgiunto dall'obiettivo di garantire contestualmente un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati dalla Pubblica amministrazione.

---

[57] https://www.governo.it/sites/governo.it/files/PNRR.pdf

[58] Con almeno 50 interventi di potenziamento delle capacità cyber della PA a protezione dei dati e dei servizi dei cittadini.

[59] Nei tempi più recenti le minacce cibernetiche hanno conosciuto uno sviluppo esponenziale sia in quantità che qualità. Il contrasto delle minacce è diventata, quindi, un'esigenza fondamentale della PA, in quanto la protezione dei dati rappresenta il presupposto necessario per far crescere, sempre più, la fiducia di cittadini e imprese nei servizi digitali erogati dalla PA.

Conseguentemente nella M1C1 si pone l'esigenza di attuare un percorso di razionalizzazione delle infrastrutture per garantire la sicurezza dei servizi erogati dalle amministrazioni mediante la migrazione diretta a *data center* più sicuri e verso infrastrutture e servizi *cloud qualificati*, ovvero conformi a standard di qualità, sicurezza, performance e scalabilità, portabilità e interoperabilità[60].

Il quadro normativo vigente in merito alla *Strategia nazionale di Cybersicurezza* (in particolare all'art. 6 del D.lgs. 18 maggio 2018, n. 65[61]) affida al Presidente del Consiglio dei ministri adotta, sentito il *Comitato interministeriale per la cyber sicurezza*[62], la definizione della *Strategia nazionale per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale*. La trasformazione digitale della PA necessita, infatti, di importanti misure di rafforzamento delle difese cyber, a partire dalla piena attuazione della disciplina in materia di "*Perimetro di Sicurezza Nazionale Cibernetica*[63]".

Detto provvedimento in questione individua, nell'ambito della strategia nazionale di cybersicurezza, obiettivi e priorità in materia di sicurezza delle reti e dei sistemi informativi. In tale sede sono, altresì, indicati il quadro di *governance*[64] per il conseguimento degli obiettivi e delle priorità sulle quali impattano le misure del PNRR.

Vengono, inoltre, contemplati i programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi, i piani di ricerca e sviluppo e un piano di valutazione dei rischi con l'elenco dei vari attori coinvolti nell'attuazione. Nella prospettiva d'attuazione, **l'Agenzia per la Cybersicurezza Nazionale** (ACN), in stretto contatto con l'Amministrazione titolare, il Dipartimento per la Trasformazione Digitale (DTD), curerà l'attuazione dell'investimento connettendo il mondo della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. La trasformazione digitale della PA contiene anche importanti misure di rafforzamento delle difese cyber, a partire dalla piena attuazione della disciplina in materia di "Perimetro di Sicurezza Nazionale Cibernetica".

60 Le amministrazioni che devono attuare il processo di migrazione potranno avvalersi dei finanziamenti previsti dalla componente richiamata per un ammontare complessivo di 1,9 miliardi di euro, nello specifico con i due investimenti che mirano all'adozione dell'approccio Cloud first da parte della PA, ovvero "Investimento 1.1: Infrastrutture digitali" e "Investimento 1.2: Abilitazione e facilitazione migrazione al cloud"

61 Come novellato dall'art. 15, comma 1 lett. f) del D.L. 14 giugno 2021, n. 82.

62 Istituito dall'art. 4, D.L. n. 82/2021 presso la Presidenza del Consiglio dei ministri, con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

63 Istituito dall'art. 1 del D.L. 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 (cfr. *infra*).

64 Inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti e le misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato.

In tale ambito è compito dell'Agenzia per la Cybersicurezza Nazionale curare l'evoluzione dell'infrastruttura e dei servizi per l'attuazione della strategia cyber nazionale che si articola su tre pilastri:

a) sviluppare le capacità di *cyber resilience* in modo diffuso nel Paese;
b) rafforzare le capacità nazionali di scrutinio e certificazione tecnologica;
c) potenziare le capacità cyber della Pubblica Amministrazione.

Capitolo IV: Soggetti, infrastrutture, definizione e disciplina del perimetro di sicurezza nazionale cibernetica

4.1. Il perimetro di sicurezza nazionale cibernetica

L'art. 1 del D.L. 21 settembre 2019, n. 105 *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 istituisce il **c.d. *perimetro di sicurezza nazionale cibernetica* quale strumento teso ad assicurare *un livello elevato di sicurezza* di reti, sistemi informativi e servizi informatici dei soggetti pubblici e privati**[65] da cui dipende:

- l'esercizio di una funzione essenziale dello Stato[66];
- la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale[67].

L'istituzione di un *perimetro di sicurezza nazionale cibernetica*, grazie anche agli oneri cui sono sottoposti i soggetti che ne fanno parte (cfr. *infra*) **costituisce un tassello**

[65] In particolare rientrano nel *perimetro di sicurezza nazionale cibernetica* le amministrazioni pubbliche, gli enti e gli operatori pubblici e privati aventi una sede nel territorio nazionale, individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici – interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro – dalle Amministrazioni competenti nei rispettivi settori.
[66] Si tratta di tutti i 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 internazionale, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario, e dei trasporti.
[67] Rientrano in quest'ambito i soggetti che realizzano:
- attività strumentali all'esercizio di funzioni essenziali dello Stato;
- attività necessarie per l'esercizio e il godimento dei diritti fondamentali;
- attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica;
- attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale.

fondamentale nello sviluppo e nel consolidamento dell'*architettura italiana di cyber security*.

Il secondo comma dell'art. 1 affida ad un decreto del Presidente del Consiglio dei ministri:

a) la definizione di modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica. L'elencazione di tali soggetti è contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, non soggetto a pubblicazione, per il quale è escluso il diritto di accesso;
b) la definizione dei criteri con i quali i soggetti preposti predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica[68];

La delega regolamentare in questione ha trovato attuazione con l'emanazione del D.P.C.M.30 luglio 2020, n. 131 *Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*.

4.2 L'individuazione delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica

Gli artt. 2 e 3 del D.P.C.M. n. 131/2020, individuano i criteri soggettivi ed oggettivi per l'individuazione degli attori che esercitano funzioni essenziali e/o che prestano servizi essenziali.

Dal punto di vista soggettivo è considerato *esercente una funzione essenziale dello Stato* il soggetto a cui l'ordinamento attribuisce compiti rivolti ad assicurare:

- **la continuità dell'azione di Governo e degli Organi costituzionali**;
- **la sicurezza interna ed esterna**;
- **la difesa dello Stato**;
- **le relazioni internazionali**;

[68] All'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il *Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica* istituito, a supporto del CISR tecnico (organismo tecnico di supporto al *Comitato interministeriale per la sicurezza della Repubblica*) di cui all'art. 6 del Regolamento di cui al D.P.C.M. 30 luglio 2020, n. 131 (cfr. *infra*).

- **la sicurezza e l'ordine pubblico**;
- **l'amministrazione della giustizia**;
- **la funzionalità dei sistemi economico e finanziario e dei trasporti.**

Riguardo alla **prestazione di servizi essenziali**, sempre sotto il profilo soggettivo, la norma (art. 2, comma 1, lett. b)) chiarisce che un soggetto, pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato laddove ponga in essere:

- attività strumentali all'esercizio di funzioni essenziali dello Stato;
- attività necessarie per l'esercizio e il godimento dei diritti fondamentali;
- attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica;
- attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

Il secondo comma dell'art. 2 al fine di contemperare l'autonomia degli Organi costituzionali con le oggettive esigenze di sicurezza dispone che tali organi, ove intendano adottare, per le proprie reti e i propri sistemi informativi e servizi informatici, misure di sicurezza analoghe a quelle previste dal D.L. n. 105/2019, possono concludere per tali finalità appositi accordi con il Presidente del Consiglio dei ministri.

Sotto il **profilo oggettivo del settore di attività**, ai fini dell'inclusione nel perimetro, l'art. 3 del D.P.C.M. n. 131/2020 chiarisce che sono oggetto di individuazione, in applicazione del criterio di gradualità, **i soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni del *Comitato interministeriale per la sicurezza della Repubblica*, nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività, ove non ricompresi in quello governativo**:

a) **interno**;
b) **difesa**;
c) **spazio e aerospazio**;
d) **energia**;
e) **telecomunicazioni**;

f) **economia e finanza**;
g) **trasporti**;
h) **servizi digitali**;
i) **tecnologie critiche**, di cui all'articolo 4, paragrafo 1, lettera b), del Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019, con esclusione di quelle riferite ad altri settori di cui al presente articolo;
l) **enti previdenziali/lavoro**.

4.3 Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica

L'art. 6 del D.P.C.M. n. 131/2020 istituisce il ***Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica*** **con funzioni di supporto al *CISR tecnico***. In particolare, il *CISR tecnico* si avvale del Tavolo interministeriale:

a) per l'esercizio delle funzioni istruttorie ai fini dell'elencazione dei soggetti inclusi nel perimetro (di cui al precedente art. 5);
b) ai fini del supporto per ogni altra attività attribuita dalla normativa vigente al *CISR* o al *CISR tecnico*.

Il ***Tavolo interministeriale*** **si riunisce periodicamente, almeno una volta ogni 6 mesi**, e può essere convocato d'iniziativa del presidente o su richiesta di almeno un componente designato, in relazione alla trattazione di specifici argomenti.

Il Tavolo interministeriale **è presieduto da un vice direttore generale del *Dipartimento delle informazioni per la sicurezza presso la Presidenza del Consiglio dei ministri*** **(DIS)**, ed **è composto** da:

- **due rappresentanti di ciascuna amministrazione CISR**;
- **un rappresentante per ciascuna delle due Agenzie** (*CISR* o al *CISR tecnico*);
- **due rappresentanti degli altri Ministeri di volta in volta interessati**[69]

Possono essere chiamati a partecipare alle riunioni rappresentanti di altre pubbliche amministrazioni, nonché di enti e operatori pubblici e privati. **La partecipazione alle riunioni del Tavolo interministeriale costituisce dovere d'ufficio e non sono, pertanto, dovuti gettoni di presenza, compensi, rimborsi spese o altri emolumenti comunque denominati**.

[69] In particolare, i rappresentanti dei Ministeri interessati sono chiamati a partecipare alle riunioni, anche su loro richiesta motivata, in relazione agli argomenti da trattare, di cui almeno uno in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica.

4.3.1 La Definizione dei criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici

Ai sensi dell'art. 7, comma 2, del D.P.C.M. n. 131/2020, ricevuta la comunicazione dell'avvenuta iscrizione nell'elenco, i soggetti inclusi nel perimetro, in esito all'analisi del rischio, per ogni funzione essenziale o servizio essenziale[70] provvedono:

a) ad individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale. A tale fine sono valutati *l'impatto di un incidente sul bene ICT*[71] e le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione;
b) a predisporre l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica. In fase di prima applicazione e fino all'aggiornamento del D.P.C.M. n. 131/2020, ai sensi dell'art. 1, comma 5, del D.L. n. 105/2019, sono individuati, all'esito dell'analisi del rischio, in ossequio al principio di gradualità, i beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale o una compromissione degli stessi con effetti irreversibili sotto il profilo della integrità o della riservatezza dei dati e delle informazioni.

Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate si applica quanto previsto dall'art.1, comma 2, lettera b), del D.L. n. 105/2019. Pertanto, i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività[72]. All'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il *Tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica*. Entro sei mesi dalla data della comunicazione dell'avvenuta iscrizione nell'elenco, i soggetti pubblici e privati iscritti nell'elencazione contenuta nello specifico atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del CIC e i soggetti che intendono fornire servizi fiduciari

[70] A tal proposito si ricorda che ai sensi dell'art. 4, comma 1, lettera c) del D.P.C.M. n. 131/2020 sono considerati funzione essenziale o servizio essenziale quelli per i quali in caso di interruzione o compromissione, il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime.
[71] In termini sia di limitazione della operatività del bene stesso, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali.
[72] L'elenco in questione è comprensivo, anche, della relativa architettura e componentistica delle reti, dei sistemi informativi e dei servizi informatici inseriti

qualificati o svolgere l'attività di gestore di posta elettronica certificata trasmettono tali elenchi all'*Agenzia per la cybersicurezza nazionale*, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza[73].
L'architettura e la componentistica relative ai beni ICT individuati, sono descritte conformemente al modello predisposto, sentito il CISR tecnico, dal DIS[74], che ne cura la comunicazione ai soggetti interessati unitamente alla comunicazione dell'avvenuta iscrizione nell'elenco (art. 8, D.P.C.M. n. 131/2020).
Il decreto previsto da questa norma viene aggiornato con cadenza almeno biennale.

4.3.2 Modalità di trasmissione degli elenchi delle reti, dei sistemi informativi e dei servizi informatici

Oltre agli adempimenti testé descritti l'art. 9 del D.P.C.M. n. 131/2020 prevede che entro sei mesi dalla data della comunicazione dell'avvenuta iscrizione nell'elenco della presidenza del consiglio dei ministri, i soggetti pubblici e privati iscritti e i quelli che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata trasmettano alla *Struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione* e al *Ministero dello sviluppo economico*, gli elenchi delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza comprensivi della descrizione dell'architettura e della componentistica predisposta secondo il citato modello predisposto dal DIS, sentito il CISR tecnico. La trasmissione degli elenchi di beni ICT avviene per il tramite di una piattaforma digitale costituita presso il DIS anche per le attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al *Nucleo per la Sicurezza Cibernetica* (NSC), nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente. Queste disposizioni trovano applicazione anche rispetto all'aggiornamento degli elenchi di beni ICT.
La struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione e il Ministero dello sviluppo economico, per i profili di rispettiva competenza, accedono a tale piattaforma per lo svolgimento delle attività di ispezione e verifica istituzionali anche ai fini dell'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative.

[73] Il *Dipartimento delle informazioni per la sicurezza*, l'AISE e l'AISI ai fini dell'esercizio delle funzioni istituzionali e l'*organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione* accedono a tali elenchi per il tramite di una specifica piattaforma digitale costituita presso l'*Agenzia per la cybersicurezza nazionale* ai sensi dell'art. 9, comma 1, del D.P.C.M. n. 131/2020.
[74] Il modello contiene l'indicazione degli elementi utili alla descrizione dei beni ICT e delle relative dipendenze.

In relazione alle reti, ai sistemi informativi e ai servizi informatici connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, la struttura della Presidenza del Consiglio dei ministri competente per la innovazione tecnologica e la digitalizzazione accede alla piattaforma in questione, limitatamente alle informazioni necessarie, individuate dal modello definito dal DIS, per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative.

Nelle more di una revisione generale delle disposizioni in materia di sicurezza (cfr. *infra*) e fatta salva l'eventuale attribuzione di classifiche previste dalla legislazione vigente, l'elencazione dei soggetti iscritti nell'elenco e gli elenchi comprensivi della descrizione dell'architettura e della componentistica, nonché dell'analisi del rischio, sono trattati, conservati e trasmessi con modalità idonee a garantirne la sicurezza, mediante misure tecniche e organizzative adeguate.

4.4. La notifica degli incidenti

L'art. 1, comma 3, del D.L. n. 105/2019 prevede che entro dieci mesi dalla data di entrata in vigore della legge di conversione (L. 18 novembre 2019, n. 133), con decreto del Presidente del Consiglio dei ministri, che disciplina altresì i relativi termini e modalità attuative siano definite le procedure secondo cui i soggetti iscritti nell'elenco, **notificano gli incidenti[75] aventi impatto su reti, sistemi informativi e servizi informatici, al *Gruppo di intervento per la sicurezza informatica in caso di incidente* (*Computer Security Incident Response Team* - CSIRT) italiano[76] che inoltra tali notifiche, tempestivamente, al Dipartimento delle informazioni per la sicurezza anche per le attività demandate al *Nucleo per la sicurezza cibernetica*. Il *Dipartimento delle informazioni per la sicurezza* assicura la trasmissione delle notifiche così ricevute all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, nonché alla Presidenza del Consiglio dei ministri, se**

[75] L'art. 1, comma 1, lett. h) del D.P.C.M. 14 aprile 2021, n. 81 definisce incidente *ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici.*

[76] Il *Computer Security Incident Response Team* (CSIRT) Italiano è un organo collegiale composto da esperti di cybersecurity, istituito con l'obiettivo di massimizzare l'efficacia della prevenzione e della risposta del Paese a incidenti da cui possano derivare danni a soggetti pubblici e/o privati. A seguito della notifica il CSIRT inoltra tempestivamente al *Dipartimento delle informazioni per la sicurezza* anche per le attività demandate al *Nucleo per la sicurezza cibernetica*; il *Dipartimento delle informazioni per la sicurezza* assicura la trasmissione delle notifiche così ricevute all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, nonché alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto un fornitore di servizi fiduciari qualificati o un gestore di posta elettronica certificata, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato.

provenienti da un soggetto pubblico, da un fornitore di servizi fiduciari qualificati o da un gestore di posta elettronica certificata, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato.

Con il D.P.C.M. che disciplina le procedure per la notifica degli incidenti sono stabilite, altresì, **le misure volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea**, relative:

1) alla **struttura organizzativa preposta alla gestione della sicurezza**;

1-bis) alle **politiche di sicurezza e alla gestione del rischio**;

2) alla **mitigazione e gestione degli incidenti e alla loro prevenzione**, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;
3) alla **protezione fisica e logica e dei dati**;
4) **all'integrità delle reti e dei sistemi informativi**;
5) alla **gestione operativa**, ivi compresa la continuità del servizio;
6) al **monitoraggio**, test e controllo;
7) alla **formazione** e consapevolezza;
8) all'affidamento di **forniture di beni, sistemi e servizi** di *information and communication technology* (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale, di standard e di eventuali limiti.

All'elaborazione di tali misure, provvedono, secondo gli ambiti di competenza il Ministero delle Imprese del Made in Italy e la Presidenza del Consiglio dei ministri, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza.

Tale decreto viene aggiornato con cadenza almeno biennale.

4.5. L'affidamento di forniture di beni, sistemi e servizi ICT

Il sesto comma dell'art. 1, D.L. n. 105/2019 incarica il governo dell'emanazione di un regolamento[77] con cui disciplinare le procedure, le modalità e i termini con cui:

a) i soggetti inseriti nel perimetro della cybersicurezza nazionale che intendano procedere, anche per il tramite delle centrali di committenza[78] 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, appartenenti a categorie individuate, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, ne danno comunicazione al *Centro di valutazione e certificazione nazionale* (CVCN), istituito presso il Ministero dello sviluppo economico[79]. Entro quarantacinque giorni dalla ricezione della comunicazione (prorogabili di quindici giorni, una sola volta, in caso di particolare complessità) il CVCN può effettuare verifiche preliminari ed imporre condizioni e test di *hardware* e *software*, secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Decorso il termine di cui al precedente periodo senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento. In caso di imposizione di condizioni e test di *hardware* e *software*, i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN. I test devono essere conclusi nel termine di sessanta giorni decorsi i quali i soggetti che hanno effettuato la comunicazione possono proseguire nella procedura di affidamento[80].

---

[77] Da adottarsi ai sensi dell'art. 17, comma 1, della L. 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione dello stesso D.L. n. 105/2019.

[78] L'art. 1, comma 512, della L. 28 dicembre 2015, n. 208 (*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato*), al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, fermi restando gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente, prevede che le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione provvedano ai propri approvvigionamenti esclusivamente tramite gli strumenti di acquisto e di negoziazione di ***Consip Spa*** o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti.

[79] La comunicazione comprende anche la valutazione del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego.

[80] In relazione alla specificità delle forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero dell'interno e del Ministero della difesa, detti Ministeri possono procedere attraverso la comunicazione ai propri *Centri di valutazione accreditati* che impiegano le metodologie di verifica e di test definite dal CVCN. Non sono oggetto di comunicazione gli affidamenti delle forniture di beni, sistemi e servizi ICT destinate alle reti, ai sistemi informativi e ai servizi informatici per lo svolgimento delle attività di prevenzione, accertamento e repressione dei reati e i casi di deroga stabiliti dal medesimo regolamento con riguardo alle forniture di beni, sistemi e servizi ICT per le quali sia indispensabile procedere in sede estera, fermo restando, in entrambi i casi, l'utilizzo di beni, sistemi e servizi ICT conformi ai livelli di sicurezza stabilite dalla normativa vigente, salvo motivate esigenze connesse agli specifici impieghi cui essi sono destinati.

b) i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici assicurano al CVCN e, limitatamente agli ambiti di specifica competenza, ai *Centri di valutazione* operanti presso i Ministeri dell'interno e della difesa, la propria collaborazione per l'effettuazione delle attività di test, sostenendone gli oneri;
c) la Presidenza del Consiglio dei ministri, per i profili di pertinenza dei soggetti pubblici, dei fornitori di servizi fiduciari qualificati e dei gestori di posta elettronica certificata e il Ministero dello sviluppo economico, per i soggetti privati svolgono attività di ispezione e verifica, impartendo, se necessario, specifiche prescrizioni[81].

4.5.1 Il Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54

La delega regolamentare contenuta nel citato art. 1, comma 6 del D.L. 21 n. 105/2019, ha trovato attuazione con l'emanazione del D.P.R 5 febbraio 2021, n. 54[82] il quale definisce:

a) le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte del *Centro di Valutazione e Certificazione nazionale* (CVCN) e dei *Centri di valutazione del Ministero dell'interno e del Ministero della difesa* (CV), ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri previsti dalla legge;
b) i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione di cui alla lettera a);
c) le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi.

4.5.1.1 La Procedura di valutazione del CVCN e dei CV

[81] Nello svolgimento di tali attività di ispezione e verifica l'accesso, se necessario, a dati o metadati personali e amministrativi è effettuato in conformità a quanto previsto dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (*Regolamento generale sulla protezione dei dati* GDPR), e dal *Codice in materia di protezione dei dati personali*, di cui al D.Lgs. 30 giugno 2003, n. 196. Per le reti, i sistemi informativi e i servizi informatici connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, le attività di ispezione e verifica sono svolte, nell'ambito delle risorse umane e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché, nei casi in cui siano espressamente previste dalla legge, in tema di prevenzione e di contrasto del crimine informatico, delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti alla Presidenza del Consiglio dei ministri per i profili di competenza.
[82] D.P.R 5 febbraio 2021, n. 54 *Regolamento recante attuazione dell'articolo 1, comma 6, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.*

I soggetti inclusi nel perimetro, prima dell'avvio delle procedure di affidamento ovvero, ove non siano previste, prima della conclusione dei contratti relativi alla fornitura di beni, sistemi e di servizi ICT ne danno comunicazione al CVCN o ai CV (art. 3, D.P.R. 5 febbraio 2021, n. 54). Tale obbligo di comunicazione permane anche nel caso in cui le procedure di affidamento siano state espletate attraverso le centrali di committenza[83]. La trasmissione è effettuata in via telematica al CVCN o ai CV per le valutazioni di rispettiva competenza. I dati contenuti nelle comunicazioni sono raccolti in archivi informatici istituiti presso le Amministrazioni nelle quali operano il CVCN e i CV.

La comunicazione, oltre ai dati identificativi del soggetto incluso nel perimetro, contiene i seguenti elementi:

a) la descrizione generale dell'oggetto della fornitura;
b) l'impiego, ovvero la destinazione d'uso dell'oggetto della fornitura nell'ambito dei beni ICT;
c) la categoria di appartenenza dell'oggetto della fornitura;
d) le informazioni e i servizi che l'oggetto della fornitura deve trattare e le relative modalità di gestione;
e) le informazioni relative all'eventuale acquisizione mediante gli strumenti di acquisto e di negoziazione di Consip Spa o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti.

In aggiunta a tali elementi la comunicazione include il documento di analisi del rischio associato all'oggetto della fornitura, anche in relazione all'ambito di impiego[84]. Le metodologie

---

[83] Le centrali di committenza sono amministrazioni aggiudicatrici o enti aggiudicatori che svolgono in via permanente attività di centralizzazione delle committenze riguardanti:
- l'acquisizione di forniture o servizi destinati a stazioni appaltanti;
- l'aggiudicazione di appalti e/o la conclusione di accordi quadro per lavori, forniture o servizi destinati a stazioni appaltanti.

Esse, inoltre, svolgono attività di committenza ausiliarie, di supporto alle attività di committenza quali:
- infrastrutture tecniche tali da permettere alle stazioni appaltanti l'aggiudicazione di appalti pubblici e/o la conclusione di accordi quadro per lavori, forniture o servizi;
- supporto e consulenza su svolgimento e progettazione delle procedure di appalto;
- predisposizione e gestione delle procedure di appalto in nome e per conto della stazione appaltante interessata.

L'art. 62, comma 7, del D.Lgs. 31 marzo 2023, n. 36, precisa che esse, in relazione ai requisiti di qualificazione posseduti:
a) progettano, aggiudicano e stipulano contratti o accordi quadro per conto delle stazioni appaltanti non qualificate;
b) progettano, aggiudicano e stipulano contratti o accordi quadro per conto delle stazioni appaltanti qualificate;
c) progettano, aggiudicano e stipulano convenzioni e accordi quadro ai quali le stazioni appaltanti qualificate e non qualificate possono aderire per l'aggiudicazione di propri appalti specifici;
d) istituiscono e gestiscono sistemi dinamici di acquisizione e mercati elettronici di negoziazione;
e) eseguono i contratti per conto delle stazioni appaltanti non qualificate qualora non siano qualificate per l'esecuzione.

Il successivo art. 63, tra le altre cose, precisa che Ogni stazione appaltante o centrale di committenza può effettuare le procedure corrispondenti al livello di qualificazione posseduto e a quelli inferiori.

[84] Il documento contiene la descrizione dei seguenti elementi:

per la predisposizione del documento di analisi del rischio e per l'individuazione dei livelli di severità dei test di corretta implementazione delle funzionalità di sicurezza e di intrusione a supporto dell'analisi di vulnerabilità sono definite con specifico atto del CVCN[85].

Il CVCN o i CV svolgono, secondo le rispettive competenze, il procedimento di verifica e valutazione dell'analisi documentale contenuta nella comunicazione (art. 4, D.P.R. n. 54/2021).

Il procedimento di verifica e valutazione dell'analisi documentale si articola nelle seguenti fasi:

a) verifiche preliminari[86];
b) fase di preparazione all'esecuzione dei test;
c) esecuzione dei test di *hardware* e di *software*[87].

All'esito delle verifiche e dei test, il CVCN o i CV, con apposito provvedimento, definiscono eventuali condizioni e test di *hardware* e di *software* da inserire nelle clausole del bando di gara o del contratto nonché eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro.

Ai fini dello svolgimento dei test di cui sub c), il CVCN può avvalersi di *laboratori accreditati di prova* (LAP) e si coordina, ove previsto, con i centri di valutazione del Ministero dell'Interno e del Ministero della Difesa.

Il CVCN condivide con i CV e i LAP le metodologie per l'effettuazione dei test ai sensi della normativa tecnica emanata con specifico decreto del Presidente del Consiglio dei ministri[88]. Il CVCN, i CV e i LAP assicurano, anche con strumenti adeguati, la riservatezza di tali metodologie.

---

a) l'ambiente operativo dell'ambito di impiego specificando:
   1. i componenti con i quali l'oggetto della fornitura interagisce e le configurazioni di tali componenti;
   2. le eventuali misure di sicurezza esistenti di tipo fisico, tecnico, procedurale, relative al personale con indicazione delle eventuali certificazioni o verifiche eseguite;
b) i requisiti di sicurezza che caratterizzano l'impiego dell'oggetto della fornitura, espressi in termini di capacità di proteggere la disponibilità, l'integrità e la riservatezza delle informazioni e i servizi.

[85] A tal fine, il CVCN, sulla base di standard tecnici di riferimento, tiene conto dell'impatto di violazioni intenzionali o accidentali sui requisiti di sicurezza che determinano eventi di indisponibilità, malfunzionamento e compromissione della funzione essenziale o del servizio essenziale.

[86] Le attività di verifica preliminare sono svolte entro il termine di quarantacinque giorni dalla comunicazione dell'avvio delle procedure di affidamento o prima della conclusione dei contratti relativi alla fornitura di beni.
Tale termine è prorogabile una sola volta, di quindici giorni, nei casi di particolare complessità, nell'ipotesi in cui l'oggetto di valutazione:
a) sia costituito da beni, sistemi e servizi ICT integrati tra di loro;
b) sia basato su tecnologie di recente sviluppo per le quali non si dispone di metodologie di test consolidate;
c) interagisce con componenti che erogano altre funzioni essenziali o servizi essenziali.
Decorsi inutilmente tali termini, senza che il CVCN o i CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire nella procedura di affidamento.

[87] 5. I test si concludono entro sessanta giorni a partire dalla data in cui il soggetto incluso nel perimetro comunica che l'oggetto della valutazione è reso fisicamente disponibile per i test al CVCN o ai CV. Decorso inutilmente tale termine, senza che il CVCN o i CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire l'esecuzione del contratto.

[88] Adottato in attuazione dell'art. 1, comma 7, lettera b), del D.L. n. 105/2019, che fissa i criteri per l'accreditamento dei laboratori.

Gli atti del procedimento di verifica e valutazione sono adottati nel rispetto dell'esigenza di tutela della sicurezza nazionale per le finalità di cui all'art. 1, comma 1, del D.L. n. 105/2019[89].

– Verifiche preliminari, individuazione di condizioni e test

Le attività di verifica preliminare, individuazione di condizioni e test si apre con la comunicazione di avvio delle procedure di affidamento, a seguito della quale il CVCN o i CV effettuano le verifiche preliminari ed eventualmente richiedono al soggetto incluso nel perimetro le informazioni necessarie per assicurare la collaborazione ai fini dell'individuazione delle condizioni per il fornitore e della tipologia di test di *hardware* e di *software* da eseguire (art. 5, D.P.R. n. 54/2021). In caso di incompletezza o incongruenza delle informazioni fornite dal soggetto incluso nel perimetro i termini di conclusione del procedimento sono sospesi, per una sola volta, fino al ricevimento delle informazioni richieste.

Il CVCN e i CV possono richiedere l'esecuzione delle seguenti tipologie di test:

a) test di corretta implementazione delle funzionalità di sicurezza allo scopo di verificare che queste ultime si comportino secondo le relative specifiche di progetto;
b) test di intrusione a supporto dell'analisi di vulnerabilità.

Nel caso di imposizione di test, il fornitore è tenuto ad effettuare almeno le seguenti attività propedeutiche e indispensabili alla loro esecuzione:

a) fornire evidenza dell'idoneità delle funzioni di sicurezza e delle loro configurazioni a soddisfare i requisiti di sicurezza;
b) provvedere all'allestimento di un ambiente di test adeguatamente rappresentativo della realtà di esercizio presso il laboratorio o, se necessario, presso il fornitore o presso il soggetto del perimetro;
c) fornire una descrizione generale dell'architettura dell'oggetto di valutazione e delle sue funzioni;
d) fornire una descrizione delle funzionalità di sicurezza implementate nell'oggetto di valutazione;
e) fornire una descrizione dei test funzionali e di sicurezza già eseguiti dal fornitore o dal produttore o da una parte terza, comprensivi dei relativi risultati.

[89] A tal proposito appare utile ricordare che la norma richiamata (l'art. 1, comma 1, del D.L. n. 105/2019) istituisce il perimetro di sicurezza nazionale cibernetica al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Il CVCN e i CV definiscono, con apposito provvedimento, da comunicarsi al soggetto incluso nel perimetro le eventuali ulteriori condizioni, i test da eseguire ed eventuali indicazioni per il supporto da parte del fornitore ai fini dell'integrazione nei bandi di gara o nei contratti con clausole che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test.

Nei bandi di gara o nei contratti, i requisiti di sicurezza dell'oggetto di fornitura sono indicati dal soggetto incluso nel perimetro adottando se necessario le opportune cautele di riservatezza, anche nei casi in cui l'acquisizione avvenga attraverso le centrali di committenza.

Il soggetto incluso nel perimetro, successivamente all'aggiudicazione della gara o della stipula del contratto, comunica al CVCN o ai CV, in via telematica, i riferimenti del fornitore e ogni elemento utile ad individuare in modo univoco l'oggetto di fornitura.

– La Preparazione all'esecuzione dei test

A seguito della comunicazione dei riferimenti del fornitore il CVCN e i CV verificano, ai sensi dell'art. 6 del D.P.R. n. 54/2021, attraverso una piattaforma informatica operante presso il Ministero dello sviluppo economico, se l'oggetto di fornitura è stato già sottoposto a precedenti valutazioni o se siano in corso valutazioni. Nel caso in cui:

a) l'oggetto sia stato sottoposto a precedenti valutazioni o sia in corso di valutazione, sono effettuate le verifiche finalizzate a evitare la duplicazione di test eventualmente già eseguiti[90];
b) l'oggetto non sia stato sottoposto a precedenti valutazioni e non sia in corso di valutazione, il CVCN o i CV, se necessario in collaborazione con il soggetto incluso nel perimetro, identificano i test da eseguire escludendo quelli precedentemente eseguiti o in corso di esecuzione.

Inoltre, nei casi *sub* b):

a) il CVCN può affidare l'esecuzione dei test ad un laboratorio accreditato, informandone il soggetto incluso nel perimetro e il fornitore;
b) il CVCN e i CV invitano il fornitore a predisporre le attività preliminari all'esecuzione dei test e definiscono la sede in cui svolgere tali attività.

[90] In tali casi sull'oggetto di valutazione non sono effettuati test nei casi in cui:
a) su tutte le funzioni di sicurezza necessarie per soddisfare i requisiti di sicurezza di interesse nella nuova valutazione siano stati eseguiti o siano in corso di esecuzione sia i test di corretta implementazione, sia i test di intrusione;
b) i test di intrusione siano stati eseguiti o siano in corso di esecuzione con riferimento a livelli di severità non inferiori a quelli selezionati per la valutazione in corso.
c) nei rimanenti casi il CVCN o i CV, se necessario in collaborazione con il soggetto incluso nel perimetro, identificano i test da eseguire escludendo quelli precedentemente eseguiti o in corso di esecuzione.

– L'Esecuzione dei test

Ai sensi dell'art. 7, una volta concluse le attività preliminari il CVCN o i CV comunicano l'avvio dei test al soggetto incluso nel perimetro e al fornitore. I test si concludono entro sessanta giorni a partire dalla data in cui il soggetto incluso nel perimetro comunica che l'oggetto della valutazione è reso fisicamente disponibile per i test al CVCN o ai CV.

Con la comunicazione di avvio dei test il CVCN o i CV specificano le modalità di collaborazione dei fornitori durante l'esecuzione delle prove[91].

Nel caso in cui si verifichi un malfunzionamento dell'oggetto di valutazione o dell'ambiente di test predisposto dal fornitore che renda impossibile o difficoltosa l'esecuzione dei test, il CVCN o i CV comunicano tempestivamente al soggetto incluso nel perimetro informando anche il fornitore, i motivi che ostano al proseguimento dei test[92].

Entro il termine di dieci giorni dalla ricezione della comunicazione, il fornitore può provvedere a risolvere il malfunzionamento. La predetta comunicazione sospende i termini per la conclusione dei test (di cui all'art. 4, comma 5, del D.P.R. n. 54/2021) che iniziano nuovamente a decorrere dalla data di soluzione del malfunzionamento verificata dal CVCN o dai CV.

In caso di eventuale mancata soluzione entro il termine, il CVCN o i CV comunicano al soggetto incluso nel perimetro e al fornitore l'impossibilità di proseguire l'esecuzione dei test e concludono il procedimento indicando la motivazione.

Il CVCN, i CV e i LAP redigono un rapporto di prova nel quale sono indicati in dettaglio l'ambiente di test, le prove eseguite ed i relativi esiti.

I LAP, eventualmente incaricati per l'esecuzione dei test, trasmettono il rapporto di prova al CVCN entro sette giorni lavorativi dalla scadenza dei termini per l'esecuzione dei test. Nel caso in cui sia stato incaricato il LAP e si verifichi un malfunzionamento dell'oggetto di valutazione

---

[91] I test sono eseguiti, secondo le metodologie predisposte dal CVCN, presso i laboratori del CVCN, dei CV e dei LAP. I CV e i LAP sono tenuti a non divulgare tali metodologie Se necessario, i test possono essere eseguiti da personale del CVCN, dei CV e dei LAP presso il fornitore o il soggetto incluso nel perimetro.

[92] La comunicazione viene effettuata nel rispetto dei principi in tema di Comunicazione dei motivi ostativi all'accoglimento dell'istanza di cui all'art. 10-*bis* della L. 7 agosto 1990, n. 241. Nello specifico questa norma prevede che *nei procedimenti ad istanza di parte il responsabile del procedimento o l'autorità competente, prima della formale adozione di un provvedimento negativo, comunica tempestivamente agli istanti i motivi che ostano all'accoglimento della domanda. Entro il termine di dieci giorni dal ricevimento della comunicazione, gli istanti hanno il diritto di presentare per iscritto le loro osservazioni, eventualmente corredate da documenti. La comunicazione di cui al primo periodo sospende i termini di conclusione dei procedimenti, che ricominciano a decorrere dieci giorni dopo la presentazione delle osservazioni o, in mancanza delle stesse, dalla scadenza del termine di cui al secondo periodo. Qualora gli istanti abbiano presentato osservazioni, del loro eventuale mancato accoglimento il responsabile del procedimento o l'autorità competente sono tenuti a dare ragione nella motivazione del provvedimento finale di diniego indicando, se ve ne sono, i soli motivi ostativi ulteriori che sono conseguenza delle osservazioni. In caso di annullamento in giudizio del provvedimento così adottato, nell'esercitare nuovamente il suo potere l'amministrazione non può addurre per la prima volta motivi ostativi già emergenti dall'istruttoria del provvedimento annullato. Le disposizioni di cui al presente articolo non si applicano alle procedure concorsuali e ai procedimenti in materia previdenziale e assistenziale sorti a seguito di istanza di parte e gestiti dagli enti previdenziali. Non possono essere addotti tra i motivi che ostano all'accoglimento della domanda inadempienze o ritardi attribuibili all'amministrazione.*

o dell'ambiente di test predisposto dal fornitore, lo stesso LAP informa tempestivamente il CVCN che procede ai sensi del comma 5.

– Esito della valutazione e prescrizioni di utilizzo

Il CVCN e i CV redigono il *rapporto di valutazione* contenente l'esito dei test sulla base del rapporto di prova.

Il rapporto di valutazione è comunicato al soggetto incluso nel perimetro e al fornitore entro sessanta giorni.

In caso di esito negativo del rapporto di valutazione, il CVCN e i CV, previa comunicazione dei motivi ostativi all'accoglimento dell'istanza, comunicano al soggetto incluso nel perimetro e al fornitore il provvedimento negativo motivato.

Nel caso di esito positivo, il CVCN può imporre al soggetto incluso nel perimetro prescrizioni per l'utilizzo dell'oggetto dell'affidamento. Tali prescrizioni possono riguardare anche il mantenimento nel tempo del livello di sicurezza nell'ambiente di esercizio.

4.5.1.2 I Casi di deroga

Ai sensi dell'art. 10 del D.P.R. n. 54/2021 e dell'art. 1, comma 6, ultimo periodo, del D.L. n. 105/2019, non sono tenute agli obblighi di comunicazione testé illustrati Autorità di pubblica sicurezza e le forze di polizia.

Ai fini della deroga alla *Comunicazione di 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 (di cui all'art. 3) è considerato indispensabile procedere in sede estera, salvo motivate esigenze connesse a specifici impieghi, per le forniture dei seguenti beni, sistemi e servizi ICT, se acquisite e utilizzate nel Paese in cui i soggetti del perimetro operano, tramite uffici, sedi o filiali all'estero:

a) realizzazione e aggiornamento di reti informatiche e di telecomunicazioni;
b) servizi di connettività;
c) servizi di gestione, assistenza e manutenzione di apparati e sistemi informatici, di rete e di telecomunicazione, erogati in presenza presso la sede estera.

L'elenco e la documentazione relativa agli affidamenti effettuati sono resi disponibili per le verifiche e le ispezioni di cui al capo IV del presente decreto.

4.5.1.3 Categorie di tipologie di beni, sistemi e servizi ICT

L'art. 13, comma 1, del D.P.R. n. 54/2021 precisa che le categorie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN o dai CV sono individuate sulla base dell'esecuzione o svolgimento delle seguenti funzioni:

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.

Le categorie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN o dai CV sono individuate con decreto del Presidente del Consiglio dei ministri sulla base dei criteri descritti nei punti da a) a f).

4.5.1.4 Le Ispezioni e le verifiche

Il capo IV (artt. da 14 a 20) del D.P.R. n.54/2021 disciplina l'attività ispettiva[93] e di verifica[94] sull'attività dei soggetti inclusi nel perimetro della cybersicurezza.

Il citato art. 14 chiarisce che le verifiche e le ispezioni hanno lo scopo di accertare l'adempimento da parte dei soggetti inclusi nel perimetro dei seguenti obblighi:

a) predisposizione, aggiornamento e trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici;
b) notifica al CSIRT italiano (*Computer Security Incident Response Team*) degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici nei termini e con le modalità previste dalla normativa tecnica;
c) adozione delle misure di sicurezza prescritte dalla legge e dalla normativa tecnica;

[93] L'art. 1, comma 1, lett. v) del dal D.P.R. n. 54/2019 definisce l'ispezione come l'*attività di tipo ricognitivo e valutativo che si articola nell'analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto utili ad accertare l'adempimento degli obblighi previsti dal D.L. n. 105/2019*.
[94] L'art. 1, comma 1 lett. u) del D.P.R. 5 febbraio 2021, n. 54 definisce la verifica come l'*attività di analisi e controllo documentale delle evidenze al fine di accertare l'adempimento degli obblighi previsti dal D.L. n. 105/2019*.

d) invio al CVCN nei termini e con le modalità previste dalla normativa tecnica della *Comunicazione di 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;
e) impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici in conformità alle condizioni e con superamento dei test imposti dal CVCN;
f) collaborazione per l'effettuazione delle attività di test da parte di fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici;
g) osservanza delle prescrizioni formulate dalle autorità competenti all'esito delle attività di ispezione e verifica;
h) osservanza delle prescrizioni di utilizzo fornite dal CVCN al soggetto.

Dette attività di verifica e ispezione sono svolte:

a) dalla *struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la digitalizzazione*, per i profili di pertinenza dei soggetti pubblici inclusi nel perimetro e dei soggetti che intendono fornire servizi fiduciari qualificati o svolgere l'attività di gestore di posta elettronica certificata.
b) dalla *struttura competente in materia di tecnologie delle comunicazioni e di sicurezza informatica del Ministero dello sviluppo economico* per i soggetti privati inclusi nel perimetro;
c) dalle *strutture specializzate* previste dalla legge (art. 1, comma 6, lettera c), del D.L. n. 105/2019), secondo le rispettive competenze, limitatamente alle reti, ai sistemi informativi, ai servizi informatici, connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica, alla difesa civile e alla difesa e sicurezza militare dello Stato, che comunicano gli esiti alla Presidenza del Consiglio dei Ministri per i profili di competenza.

Ai fini dello svolgimento delle verifiche e delle ispezioni, le autorità competenti individuano, nel rispetto dei criteri di professionalità e rotazione, il personale incaricato, nonché un responsabile del procedimento ai sensi dell'art. 6 della L. n. 241/1990[95].
Ai sensi dell'art. 16, le autorità competenti dispongono verifiche e ispezioni sulla base degli atti di programmazione adottati, nonché in caso di esigenze derivanti da notifiche di incidenti,

[95] Al momento dell'accettazione dell'incarico, il personale incaricato dichiara di non trovarsi, per quanto a sua conoscenza, in una situazione di conflitto di interessi e si impegna a segnalare ogni sopravvenuta situazione di conflitto, anche potenziale.

inadempimenti rilevati degli obblighi di legge e segnalazioni provenienti da altre Autorità Pubbliche.
Le ispezioni sono svolte anche successivamente alle verifiche qualora si ritenga necessario riscontrare le evidenze acquisite, oppure qualora le predette verifiche presentino elementi tali da richiedere un approfondimento.

Il responsabile del procedimento comunica ai soggetti interessati di cui all'art. 7, comma 1, della L. n. 241/1990[96], inclusi nel perimetro, l'avvio del procedimento di verifica o di ispezione, richiedendo le informazioni e la documentazione necessaria al fine dell'espletamento delle relative attività.
I destinatari di tale comunicazione nominano un incaricato in possesso di professionalità e di competenze nella materia della sicurezza cibernetica, quale unico referente per lo svolgimento delle attività di verifica ed ispezione, comunicandone il nominativo al responsabile del procedimento.
I procedimenti di verifica ed ispezione, si concludono, rispettivamente:

- entro il termine di centoventi giorni dalla data della comunicazione dell'avvio del procedimento di verifica;
- entro il termine di novanta giorni dalla data della comunicazione l'avvio del procedimento di ispezione.

All'esito delle attività di verifica e di ispezione le autorità competenti possono formulare specifiche prescrizioni a cui i soggetti inclusi nel perimetro devono attenersi. Il rispetto delle prescrizioni può essere oggetto, a sua volta, di attività di verifica e ispezione.

– L'attività di verifica

Le verifiche sono effettuate mediante analisi e controllo documentale delle evidenze e di ogni altro elemento di fatto e di diritto, al fine di accertare l'adempimento degli obblighi previsti dal decreto-legge e dai relativi decreti attuativi (art. 17). Il procedimento di verifica è avviato con la comunicazione di avvio del procedimento (cfr. *supra*). I soggetti destinatari della comunicazione rendono disponibile la documentazione richiesta ai fini delle attività di verifica, entro quindici giorni dalla ricezione della comunicazione.
Durante l'esecuzione delle attività di verifica, il responsabile del procedimento, qualora le evidenze risultino incomplete o incongruenti, può richiedere chiarimenti e integrazioni che

[96] Soggetti nei confronti dei quali il provvedimento finale è destinato a produrre effetti diretti inclusi quelli che per legge debbono intervenire nel procedimento.

sono resi entro dieci giorni dalla ricezione della richiesta, secondo le modalità indicate dal richiedente. Dell'attività svolta nel corso delle verifiche è redatto apposito verbale che il personale incaricato trasmette al responsabile del procedimento.
Qualora nel corso della verifica vengano in rilievo evidenze di fatti che possono integrare violazioni di disposizioni normative rientranti nelle attribuzioni istituzionali di altre Amministrazioni, il personale incaricato ne dà conto nel verbale e l'autorità competente trasmette senza ritardo alle Amministrazioni competenti la relativa documentazione.

– L'attività ispettiva

Le ispezioni, ai sensi dell'art. 18, possono essere svolte mediante:

a) riscontro delle evidenze eventualmente acquisite in sede di verifica, qualora le stesse presentino elementi meritevoli di approfondimento;
b) analisi, rilevazione, acquisizione e verifica di conformità di elementi di fatto e di diritto ritenuti necessari.

Il personale incaricato, per lo svolgimento di tali attività, può richiedere o eventualmente acquisire direttamente tutte le evidenze ritenute utili ai fini dell'accertamento.
Le ispezioni possono essere effettuate presso le sedi utilizzate dai soggetti inclusi nel perimetro nei casi di notifiche di incidenti, inadempimenti rilevati degli obblighi di legge e segnalazioni provenienti da altre Autorità Pubbliche. Il relativo procedimento è avviato con la *comunicazione di avvio del procedimento* (cfr. *supra*), con un preavviso non inferiore a quindici giorni. L'informativa riporta:

a) le date e i siti in cui sarà effettuata l'ispezione;
b) le persone da intervistare o i loro ruoli e responsabilità;
c) le reti, i sistemi informativi e i servizi informatici da sottoporre a ispezione;
d) i nominativi del personale incaricato;
e) eventuali altre informazioni utili ai fini dell'ispezione.

Entro cinque giorni dalla ricezione della comunicazione di avvio del procedimento ispettivo, il soggetto ricevente può proporre date alternative a quelle previste per l'ispezione, individuando un termine non superiore a dieci giorni per il differimento dell'ispezione. Qualora il soggetto proponga date alternative, l'autorità competente può:

a) accettare la proposta di modifica delle date, inviando una comunicazione almeno sette giorni prima della prima data prevista per l'ispezione;
b) proporre ulteriori date e comunicarle al soggetto inviando, anche in questo caso, una comunicazione almeno sette giorni prima della prima data prevista per l'ispezione. Tali nuove date non possono essere soggette a richieste di modifica e si intendono, quindi, confermate.

Almeno cinque giorni prima dell'ispezione prevista, il soggetto sottoposto alla stessa comunica il nominativo del referente unico per lo svolgimento delle attività di ispezione (di cui all'art. 16, comma 4, del D.P.R. n. 54/2021)

Durante l'ispezione, i soggetti inclusi nel perimetro mettono a disposizione tutte le risorse umane richieste, necessarie per agevolare le relative attività, garantendo altresì l'accesso ai locali, ai dispositivi e alle informazioni rilevanti ai fini dell'ispezione, anche se non esplicitamente e preventivamente indicati nella comunicazione di avvio del procedimento ispettivo. Qualora durante il corso dell'ispezione emergano evidenze meritevoli di approfondimento, le stesse possono essere esaminate in una fase successiva.

Dell'attività svolta nel corso dell'ispezione è redatto apposito processo verbale da parte del personale incaricato che lo sottoscrive unitamente al referente unico per lo svolgimento delle attività di ispezione a ciò incaricato. Nel caso in cui quest'ultimo si rifiuti di sottoscrivere il verbale, il personale incaricato ne dà evidenza nel verbale. Una copia del verbale è comunque rilasciata al referente unico, e una copia è trasmessa al responsabile del procedimento.

Qualora nel corso dell'ispezione vengano in rilievo evidenze di fatti che possono integrare violazioni di disposizioni normative rientranti nelle attribuzioni istituzionali di altre Amministrazioni, il personale incaricato ne dà conto nel verbale e l'autorità competente trasmette senza ritardo alle Amministrazioni competenti la relativa documentazione.

– Gli esiti delle attività di verifica e di ispezione

L'autorità competente, raccolti gli esiti delle attività di verifica e di ispezione, adotta il provvedimento di conclusione del procedimento, impartendo, se necessario, specifiche prescrizioni e dandone comunicazione all'interessato. Nei casi previsti, l'autorità competente avvia il procedimento per l'applicazione delle sanzioni di previste dall'articolo 1, comma 9, del D.L. n. 105/2019 (cfr. *infra*).

4.5.2 Il Decreto del presidente del Consiglio del Ministri 15 giugno 2021

La delega regolamentare contenuta nell'art. 1, comma 6, D.L. 21 n. 105/2019, con particolare riferimento alla lett. a) in materia di *individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica*, ha trovato ulteriore specificazione ad opera del D.P.C.M. 15 giugno 2021[97], che integra le disposizioni del regolamento adottato con il D.P.R. n. 54/2021.

[97] DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 15 giugno 2021 *Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in*

In particolare, il D.P.C.M. 15 giugno 2021 individua le categorie in relazione alle quali i soggetti inclusi nel perimetro che intendano procedere[98] all'affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici delle pubbliche amministrazioni[99], effettuano la comunicazione al *Centro di valutazione e certificazione nazionale* CVCN o ai CV centri di valutazione del Ministero dell'interno e del Ministero della difesa.

L'art. 3 del D.P.C.M. chiarisce che le categorie sono individuate sulla base dei criteri tecnici di cui all'art. 13, comma 1, del D.P.R. n. 54/2021 (già esaminati nel par. 5.1.3). Inoltre, dette categorie sono contenute nell'elenco di cui all'allegato 1 dello stesso D.P.C.M. 15 giugno 2021.

ELENCO DELLE CATEGORIE (All. 1, al D.P.C.M. 15 giugno 2021)

Categoria	**Bene, sistema, servizio**
Componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione)	*Router* *Switch* *Repeater* Bilanciatori di carico *Traffic shaper* *Proxy* Ponte radio *Access Network* per reti Radiomobili 2G, 3G, 4G, 5G *Gateway Wifi* *Network Function Virtualization* (NFV): o *vSwitch* | o *vRouter* | o *Application Function* (5G) *Optical transmission board* *Multiservice Provisioning Platform* (MSPP)

attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

[98] Anche per il tramite delle centrali di committenza alle quali sono tenuti a fare ricorso.

[99] A tal proposito si ricorda che l'art. 1, comma 1 lett. i), del D.P.R. 5 febbraio 2021, n. 54 definisce servizio informatico, un servizio consistente interamente o prevalentemente nel trattamento di informazioni, per mezzo della rete e dei sistemi informativi, ivi incluso quello di *cloud computing* di cui all'art. 3, comma 1, lettera aa), del decreto legislativo 18 maggio 2018, n. 65.

	Automotive ECU switch (*Ethernet*, CAN, LIN) *IoT Edge Gateway*
Componenti *hardware* e *software* che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati	*Firewall* *Security Gateway* *Hardware Security Module* (HSM) *Intrusion Detection System* (IDS) *Intrusion Prevention System* (IPS) *Network Function Virtualization* (NFV) o *Authentication Server Function* (5G) o *Whitelisting* dei processi *Virtual Private Network* (VPN) *Trusted Platform Module*
Componenti *hardware* e *software* per acquisizione dati, monitoraggio supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali	Sistemi SCADA (*Supervisory Control And Data Acquisition*) *Manufacturing Execution Systems* (MES) *Software Defined Network* (SDN) Controller Sistemi *Artificial Intelligence* (AI) e *Machine Learning* (ML) per gestione reti/sistemi 5G *Mobile Edge Computing* (MEC) NFV: o *Network Slice Selection Function* (5G) o *Application Function* (5G)| o *Policy Control Function* (5G) o *Unified Data Management* (5G) o *Session Management Function* (5G) *Management and Orchestration* (MANO) *IoT orchestrator*
Applicativi *software* per l'implementazione di meccanismi di sicurezza	Applicazioni informatiche per la sicurezza o *Public Key Infrastructure* (PKI) o *Single Sign-On* (SSO)

	o Controllo Accessi Moduli *software* che implementano *Web Service* mediante API, per protocolli di comunicazione

Il loro aggiornamento, ad opera di specifico decreto del Presidente del Consiglio dei ministri, avviene con cadenza almeno annuale, avuto riguardo all'innovazione tecnologica, nonché all'eventuale modifica dei criteri tecnici di cui all'art. 13, comma 1, del D.P.R. n. 54/2021.

4.6. I compiti del CVCN nell'ambito dell'approvvigionamento di prodotti, processi, servizi ICT

Il settimo comma dell'art. 1, D.L. n. 105/2019, precisa che nell'ambito dell'approvvigionamento di prodotti, processi, servizi ICT e associate infrastrutture destinati alle reti, ai sistemi informativi e per l'espletamento dei servizi informatici, il CVCN assume i seguenti compiti:

a) contribuisce all'elaborazione delle misure di sicurezza per ciò che concerne l'affidamento di forniture di beni, sistemi e servizi ICT;
b) definisce le metodologie di verifica e di test e svolge le attività di verifica ed ispezione ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego. Ove necessario il CVCN detta anche prescrizioni di utilizzo al committente[100];
c) elabora e adotta, previo conforme avviso del *Tavolo interministeriale* schemi di certificazione cibernetica, tenendo conto degli standard definiti a livello internazionale e dell'Unione europea, laddove, per ragioni di sicurezza nazionale, gli schemi di certificazione esistenti non siano ritenuti adeguati alle esigenze di tutela del perimetro di sicurezza nazionale cibernetica.

[100] A tali fini il CVCN si avvale anche di laboratori che esso stesso ha provveduto ad accreditare secondo criteri stabiliti da un decreto del Presidente del Consiglio dei ministri da adottarsi, su proposta del CIC, entro dieci mesi conversione in legge del D.L. n. 105/2019.

4.7. Il regime sanzionatorio

L'art. 1, comma 9, del D.L. n. 105/2019 definisce il regime sanzionatorio per le ipotesi di inosservanza degli obblighi derivanti dall'appartenenza al perimetro di cybersicurezza nazionale. In particolare, la norma prevede che, salvo che il fatto costituisca reato:

a) il mancato adempimento degli obblighi di predisposizione, di aggiornamento e di trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici è punito con la sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000;
b) il mancato adempimento dell'obbligo di notifica degli incidenti, nei termini prescritti, è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;
c) l'inosservanza delle misure di sicurezza volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici, è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;
d) la mancata comunicazione di avvio delle procedure di affidamento nei termini prescritti, è punita con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;
e) l'impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, in violazione delle condizioni o in assenza del superamento dei test imposti dal CVCN ovvero dai Centri di valutazione di cui al comma 6, lettera a), è punito con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000;
f) la mancata collaborazione per l'effettuazione delle attività di test da parte di fornitori di beni, sistemi e servizi destinati alle reti è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;
g) il mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio dei ministri in esito alle attività di ispezione e verifica è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;
h) il mancato rispetto delle prescrizioni definite dal CVCN in materia di metodologie di verifica e di test è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.

L'impiego di prodotti e di servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici in assenza della comunicazione o del superamento dei test, oltre alle sanzioni di cui ai punti d) ed e), comporta l'applicazione della sanzione amministrativa accessoria della *incapacità ad assumere incarichi di direzione, amministrazione e controllo*

nelle persone giuridiche e nelle imprese, per un periodo di tre anni a decorrere dalla data di accertamento della violazione.

Il comma 11, dell'art. 1, D.L. n. 105/2019 prevede la reclusione da uno a tre anni per chiunque, allo scopo di ostacolare o condizionare l'espletamento delle attività ispettive e di vigilanza fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi o ai fini delle comunicazioni di avvio delle procedure di affidamento, o per lo svolgimento delle attività ispettive e di vigilanza od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto.

Le autorità competenti per l'accertamento delle violazioni e per l'irrogazione delle sanzioni amministrative sono la Presidenza del Consiglio dei ministri, per i soggetti pubblici, per i fornitori di servizi fiduciari qualificati e per i gestori di posta elettronica certificata, e il Ministero dello sviluppo economico, per i soggetti privati di cui al medesimo comma. Ai fini dell'accertamento e dell'irrogazione di tali sanzioni trovano applicazione i principi generali in materia di sanzioni amministrative di cui al Capo I, Sezioni I e II, della L. 24 novembre 1981, n. 689.

Per i dipendenti dei soggetti pubblici inclusi nel perimetro di cybersicurezza nazionale, la violazione delle disposizioni di cui sin qui illustrate può costituire causa di *responsabilità disciplinare* e *amministrativo-contabile*.

La Presidenza del Consiglio dei ministri, per lo svolgimento delle funzioni in materia di perimetro della sicurezza nazionale cibernetica può avvalersi dell'*Agenzia per l'Italia Digitale* (AgID) sulla base di apposite convenzioni.

Il comma 19-*bis*, dell'art. 1, D.L. n. 105/2019 attribuisce al Presidente del Consiglio dei ministri il coordinamento della coerente attuazione delle disposizioni in materia di perimetro di sicurezza nazionale cibernetica. In questa attività il presidente del Consiglio dei Ministri può avvalersi anche del *Dipartimento delle informazioni per la sicurezza*, che assicura gli opportuni raccordi con le autorità e i soggetti coinvolti.

4.8. Le Determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica

Ai sensi dell'art. 5 del D.L. n. 105/2019, il Presidente del Consiglio dei ministri, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, su deliberazione del *Comitato interministeriale per la sicurezza della Repubblica*, *può comunque disporre*, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua

mitigazione, in deroga ad ogni disposizione vigente, nel rispetto dei principi generali dell'ordinamento giuridico e secondo un criterio di proporzionalità, *la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati*. Laddove in tali determinazioni sia recata deroga alle leggi vigenti, anche ai fini delle ulteriori necessarie misure correlate alla disattivazione o all'interruzione, le stesse determinazioni devono contenere l'indicazione delle principali norme a cui si intende derogare e tali deroghe devono essere specificamente motivate. Dette determinazioni non sono soggette) al controllo preventivo di legittimità di cui all'art. 3 della L. 14 gennaio 1994, n. 20, in materia di controllo della Corte dei conti.

Qualora il Presidente del Consiglio dei ministri eserciti poteri è tenuto ad informare, entro trenta giorni, il *Comitato parlamentare per la sicurezza della Repubblica* delle misure disposte.

Appendice I : Il D.Lgs. 3 agosto 2022, n. 123 e l'attuazione del quadro per l'introduzione di sistemi europei di certificazione

1. Premessa

Con il D.Lgs. 3 agosto 2022, n. 123 (entrato in vigore il 4 settembre 2022) sono state emanate le norme di attuazione del c.d. *Cybersecurity Act* Europeo, il Regolamento (Ue) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'*Agenzia dell'Unione europea per la cibersicurezza*, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (*regolamento sulla cibersicurezza*).

La normativa eurounitaria persegue come finalità principale quella di garantire *il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione*. A tal fine detto Regolamento stabilisce:

a) gli *obiettivi*, i *compiti* e gli *aspetti organizzativi* relativi all'ENISA, (*Agenzia dell'Unione europea per la cibersicurezza*);
b) un *quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza* al fine di garantire un livello adeguato di cibersicurezza dei prodotti TIC[101], servizi TIC e processi TIC nell'Unione, oltre che al fine di evitare la frammentazione del mercato interno per quanto riguarda i sistemi di certificazione della cibersicurezza nell'Unione.

Rispetto alla disciplina dell'ENISA il Regolamento mira ad emancipare l'Agenzia dal ruolo di mera assistenza tecnica alle Istituzioni europee e agli Stati membri nella predisposizione delle politiche in materia di sicurezza informatica per attribuirle anche un ruolo attivo nella gestione operativa degli incidenti informatici.

La definizione di un *corpus* normativo europeo comune in materia di certificazione della sicurezza delle Tecnologie dell'Informazione e della Comunicazione (prodotti, servizi e processi informatici) consente un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza fornendo regole comuni in materia di disponibilità, autenticità, integrità e la riservatezza dei dati processati (conservati, trattati, e trasmessi) e dei servizi offerti *on-line*.

La disciplina comune europea in materia di certificazione della cibersicurezza trova applicazione in materia di certificazione sia volontaria che obbligatoria.

2. Il D.Lgs. 3 agosto 2022, n. 123: funzione ed ambito di applicazione

[101] L'acronimo TIC sta ad indicare prodotti, servizi e processi realizzati attraverso la Tecnologia dell'Informazione e della Comunicazione.

Il D.Lgs. n. 123/2022 individua le misure necessarie per adeguare la normativa interna al *nuovo quadro europeo di certificazione della cibersicurezza*, introdotto mediante le disposizioni del Titolo III del citato Regolamento (UE) 2019/881.
A tal fine, il D.Lgs. n. 123/2022 prevede:

a) l'individuazione dell'organizzazione dell'*Autorità nazionale di certificazione della cybersicurezza* in Italia, di cui all'articolo 4, comma 1, in base ai compiti ed ai poteri ad essa attribuiti in materia di vigilanza in ambito nazionale e di rilascio dei certificati di *cybersicurezza*, con riferimento al quadro europeo di certificazione;
b) le modalità di cooperazione dell'*Autorità nazionale di certificazione della cybersicurezza* italiana con le altre autorità pubbliche nazionali ed europee e con l'*Organismo di accreditamento*[102];
c) la definizione di un sistema sanzionatorio applicabile in caso di violazione delle norme del quadro europeo di certificazione con sanzioni effettive, proporzionate e dissuasive.

La disciplina di attuazione del quadro per l'introduzione di sistemi europei di certificazione di cui al D.Lgs. n. 123/2022 trova applicazione generale ma restano salve le disposizioni specifiche riguardanti le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.
Rispetto all'applicazione di questa disciplina l'art. 2 chiarisce che il trattamento dei dati personali derivante dall'applicazione del D.Lgs. n. 123/2022 è effettuato ai sensi del *Regolamento Generale sulla Protezione dei Dati* GDPR (Regolamento (UE) 2016/679) e del c.d. *Codice della privacy* di cui al D.Lgs. 30 giugno 2003, n. 196.

3. La Vigilanza nazionale

L'*Agenzia per la cybersicurezza nazionale*, ai sensi dell'art. 5, realizza l'attività di vigilanza del mercato in ambito nazionale ai fini della corretta applicazione delle regole previste dai sistemi europei di certificazione della *cybersicurezza*, con riferimento ai certificati di *cybersicurezza* ed alle dichiarazioni UE di conformità emessi nel territorio dello Stato nel rispetto della normativa interna ed eurounitaria. A tal fine essa vigila su fornitori e fabbricanti emittenti le dichiarazioni UE di conformità, sui titolari di certificati europei di *cybersicurezza* e sugli

[102] L'art. 3, comma 1, lett. m) del D.Lgs. n. 123/2022 definisce l'*Organismo di accreditamento* come l'organismo autorizzato a svolgere l'attività di accreditamento nel territorio dello Stato, ai sensi dell'art. 2, par. 1, n. 11, del Regolamento (CE) 765/2008, designato con decreto del Ministro dello sviluppo economico del 22 dicembre 2009 in attuazione dell'articolo 4, comma 2, della legge 23 luglio 2009, n. 99. A tal proposito si ricorda che secondo quanto previsto dal precedente n. 10, dell'art. 2, par. 1, del Regolamento (CE) 765/2008, per *accreditamento* deve intendersi l'*attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità.*

organismi di valutazione della conformità[103]. In quest'ambito l'*Agenzia per la cybersicurezza nazionale*:

a) assiste e sostiene attivamente l'*Organismo di accreditamento* nel monitoraggio e nella vigilanza delle attività degli organismi di valutazione della conformità[104]. Le modalità di sostegno ed assistenza dell'Agenzia all'*Organismo di accreditamento* per l'attività di vigilanza sono disciplinate da apposita convenzione o protocollo di intesa fra i medesimi soggetti;
b) monitora e vigila sulle attività degli organismi di valutazione della conformità pubblici di cui all'art. 56, par. 5, lett. b), del Regolamento (UE) 2019/881[105];
c) ove previsto dal sistema di certificazione, autorizza gli organismi di valutazione della conformità e limita, sospende o revoca l'autorizzazione esistente qualora violino le prescrizioni del Regolamento medesimo, dandone notizia all'Organismo di accreditamento.

L'Agenzia, nello svolgimento dell'attività di vigilanza, opera anche in collaborazione con altre autorità di vigilanza del mercato competenti in Italia e con le autorità di vigilanza degli altri Stati membri[106]. L'Agenzia esegue l'attività di vigilanza anche in collaborazione con le Forze dell'ordine.

Nell'attività di vigilanza affidatale, l'Agenzia può effettuare, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di *cybersicurezza* e degli emittenti le dichiarazioni di conformità UE, indagini ed *audit*, ottenendo informazioni anche tramite l'accesso ai locali degli organismi di valutazione della conformità o dei titolari dei certificati europei di *cybersicurezza*, revocare certificati, irrogare sanzioni pecuniarie ed accessorie. L'attività di vigilanza dell'Agenzia può prevedere prelievi di prodotti.

---

[103] L'Agenzia, per le prove tecniche nell'ambito delle attività di vigilanza nazionale, può effettuare valutazioni di sicurezza informatica anche attraverso esperti esterni o laboratori di prova abilitati dall'Agenzia e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

[104] Resta, comunque, salvo quanto previsto dall'art. 60, par. 3, del Regolamento (UE) 2019/881 per le ipotesi in cui i sistemi europei di certificazione della cibersicurezza stabiliscono requisiti specifici o supplementari nonché quanto previsto dalle disposizioni in materia di funzioni di monitoraggio e vigilanza sulle attività degli organismi di valutazione.

[105] La norma in questione prevede che in casi debitamente giustificati, un sistema europeo di certificazione della cibersicurezza può prevedere che i certificati europei di cibersicurezza derivanti da tale sistema possano essere rilasciati unicamente da un ente pubblico. Detto ente può essere, alternativamente, uno dei due soggetti seguenti:

a) un'autorità nazionale di certificazione della cibersicurezza designata ai sensi dell'art. 58, par. 1, del Regolamento (UE) 2019/881, oppure un'autorità nazionale di certificazione della cibersicurezza stabilita in un altro Stato membro designata, a seguito di accordo con lo stesso Stato, affinché sia responsabile dei compiti di vigilanza;
b) un organismo pubblico accreditato come organismo di valutazione della conformità a norma dell'articolo 60, paragrafo.

[106] Come individuate dall'art. 58, par. 7, lett. a) ed h), del Regolamento (UE) 2019/881.

Nel caso in cui l'Agenzia, in esito alle attività di vigilanza, accerti l'emissione di un certificato non conforme, rilasciato ai sensi del Regolamento (UE) 2019/881[107], detto certificato è sottoposto a revoca:

a) per il livello di affidabilità *elevato* l'Agenzia provvede direttamente alla revoca del certificato;
b) per il livello di affidabilità di *base* o *sostanziale* nel caso in cui il certificato non conforme sia relativo ad un prodotto TIC, servizio TIC o processo TIC che ha comportato un concreto e dimostrato pregiudizio ad un servizio essenziale, ad un servizio di comunicazione elettronica, alla salute o all'incolumità personale l'Agenzia chiede all'organismo che ha emesso il certificato di provvedere alla revoca del certificato entro e non oltre cinque giorni e, in caso di inottemperanza, provvede direttamente entro i successivi cinque giorni;
c) se previsto espressamente dallo specifico sistema europeo di certificazione, si provvede in base alle regole stabilite dal sistema specifico di certificazione.

Accertata l'emissione di un certificato non conforme, in esito alle attività e fatti salvi i casi di revoca testé illustrati, l'Agenzia chiede all'organismo che ha emesso il certificato di ripetere in tutto o in parte l'attività di valutazione o di integrare tale attività con ulteriori verifiche e, quindi, di ricondurre il certificato a conformità entro centoventi giorni o revocare il certificato. In caso di mancata riconduzione a conformità o mancata revoca del certificato non conforme da parte dell'organismo, il certificato decade. La riconduzione a conformità o la revoca del certificato sono divulgate con gli strumenti e le modalità previsti dal sistema europeo di certificazione della cibersicurezza nell'ambito della propria la politica di divulgazione dei certificati europei di cibersicurezza rilasciati, modificati o revocati nell'ambito del sistema.
L'attavo comma dell'art. 5 obbliga gli organismi di valutazione della conformità, i titolari dei certificati europei di cybersicurezza e gli emittenti delle dichiarazioni di conformità durante

[107] Il riferimento è ai certificati rilasciati ai sensi dell'art. 56, par. 4, 5, lett. b), o 6, lettere a) e b), del Regolamento (UE) 2019/881. Nello specifico, il par. 4 individua due categorie di certificati, in base al livello di affidabilità, qualificati come «*di base*» o «*sostanziale*». Tale classificazione è operata sulla base dei criteri previsti dal sistema europeo di certificazione della cibersicurezza. Il successivo paragrafo 5, lett. b), derogando parzialmente i principi di cui al comma precedente prevede che, in casi debitamente giustificati, un sistema europeo di certificazione della cibersicurezza possa prevedere che i certificati europei di cibersicurezza possano essere rilasciati unicamente da un organismo pubblico accreditato come organismo di valutazione della conformità. Infine, il sesto comma dispone che, ove un sistema europeo di certificazione della cibersicurezza richieda un livello di affidabilità «*elevato*», il certificato europeo di cibersicurezza nell'ambito di tale sistema deve essere rilasciato solo da un'autorità nazionale di certificazione della cibersicurezza oppure, nei casi seguenti, da un organismo di valutazione della conformità:

a) previa approvazione dell'autorità nazionale di certificazione della cibersicurezza per ogni singolo certificato europeo dicibersicurezza rilasciato da un organismo di valutazione della conformità;
b) sulla base di una delega generale del compito di rilasciare tali certificati europei di cibersicurezza a un organismo divalutazione della conformità da parte dell'autorità nazionale di certificazione della cibersicurezza.

l'attività di vigilanza a cui sono sottoposti a cooperare con l'Agenzia nell'attività di verifica sui certificati e sulle dichiarazioni UE da essi emessi. A tal fine detti soggetti, su richiesta dell'Agenzia, devono mettere a disposizione tutti i documenti di valutazione necessari per dimostrare la conformità dei certificati e le dichiarazioni oggetto di verifica da parte dell'Agenzia assieme agli strumenti di valutazione eventualmente forniti dal fabbricante o dal fornitore nell'attività di valutazione come indicato nei rapporti di valutazione. L'onere della prova della conformità di certificati e dichiarazioni è in capo agli organismi di valutazione della conformità, ai titolari dei certificati o agli emittenti delle dichiarazioni di conformità.

4. Il Rilascio dei certificati di cybersicurezza

I certificati di cybersicurezza vengono inquadrati in una classificazione tripartita, in ragione del livello di affidabilità:

- *affidabilità di base* quanto il certificato garantisce che un prodotto TIC, servizio TIC o processo TIC è stato oggetto di valutazione ad un livello comunque sufficiente a ridurre i rischi legati ai più diffusi incidenti o attacchi informatici;
- *affidabilità sostanziale* quando il certificato garantisce l'esistenza di standard e funzionalità di sicurezza elevati, tali da limitare i rischi noti di attacchi informatici causati da soggetti dotati di abilità e risorse limitate;
- *affidabilità elevata* quando il certificato assicura che un prodotto TIC, servizio TIC o processo TIC rispetta i requisiti di sicurezza e sia stato oggetto di valutazioni mirate alla minimizzazione dei rischi derivanti da attacchi informatici.

L'Agenzia, ai sensi dell'art. 6, D.Lgs. n. 123/2022, rilascia i certificati di cybersicurezza con livello di affidabilità *elevato* tramite l'*Organismo di Certificazione della Sicurezza Informatica* (OCSI), che si può avvalere di esperti o di laboratori di prova abilitati dall'Agenzia ad operare per proprio conto e iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale, ferme restando, per specifici sistemi di certificazione, le possibili modalità di emissione dei certificati alternative (ai sensi dell'art. 56, par. 6, lettere a) e b), del Regolamento, che individuano le fattispecie in cui un sistema europeo di certificazione della cibersicurezza può richiedere un livello di affidabilità «*elevato*).

Ove uno specifico sistema di certificazione preveda il rilascio dei certificati con livello di affidabilità *sostanziale* o *di base* unicamente da parte di un organismo pubblico, l'Agenzia rilascia tali certificati attraverso l'OCSI. Il rilascio può avvenire ad opera di altro organismo di valutazione della conformità pubblico, accreditato dall'*Organismo di Accreditamento*, monitorato e vigilato dall'Agenzia nel rispetto della normativa eurounitaria e designato

dall'Agenzia con proprio provvedimento, salvo diverse disposizioni dello specifico sistema europeo di certificazione.
La certificazione della cybersicurezza è volontaria, salvo il caso in cui sia diversamente specificato dal diritto dell'Unione o dal diritto nazionale. In mancanza di un diritto dell'Unione armonizzato, l'Agenzia può adottare, previa consultazione con i portatori di interesse, regolamentazioni tecniche nazionali in cui sia prevista una certificazione obbligatoria nel quadro di un sistema europeo di certificazione della cybersicurezza (art. 6, comma 3).
Gli oneri legati al rilascio dei certificati da parte dell'Agenzia sono a carico del soggetto richiedente la certificazione.

5. Le dichiarazioni UE di conformità

In un sistema di certificazione in cui è autorizzata l'*autovalutazione di conformità* i fornitori o fabbricanti di prodotti TIC, servizi TIC o processi TIC possono rilasciare sotto la propria responsabilità dichiarazioni UE di conformità di livello di base per dimostrare il rispetto di requisiti tecnici previsti nel sistema (art. 7).
Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC rende disponibile all'Agenzia, per il periodo stabilito nel corrispondente sistema europeo di certificazione della cybersicurezza:

- la dichiarazione UE di conformità;
- la documentazione tecnica;
- tutte le altre informazioni pertinenti relative alla conformità dei prodotti TIC o servizi TIC al sistema.

Una copia della dichiarazione UE di conformità è, inoltre, trasmessa all'Agenzia e all'ENISA.

Nel caso in cui l'Agenzia, in esito alle attività di vigilanza, accerti la non conformità di una dichiarazione UE di conformità sorge in capo al fabbricante (o al fornitore o emittente) l'obbligo di revisionare o revocare la dichiarazione stessa entro trenta giorni, dandone comunicazione all'Agenzia e all'ENISA, salvo diversa disposizione dello specifico sistema di certificazione.
Il quarto comma dell'art. 7 ribadisce il principio di cui all'art. 53, par. 4 del Regolamento (UE) 2019/881 secondo cui il rilascio di una dichiarazione UE di conformità è volontario, salvo in caso in cui sia diversamente specificato dalla normativa interna o da quella europea. In mancanza di un diritto dell'Unione armonizzato, l'Agenzia può stabilire, previa consultazione con i portatori di interesse, l'obbligatorietà della dichiarazione UE di conformità nelle fattispecie di cui all'art. 6, comma 3 (cfr. *supra*).

6. L'accreditamento e l'autorizzazione degli organismi di valutazione della conformità e l'abilitazione dei laboratori di prova ed esperti dell'Agenzia

Ai sensi dell'art. 8, comma 1 del D.Lgs. n. 123/2022, l'*Organismo di accreditamento*, nello svolgimento dei compiti relativi all'accreditamento degli organismi di valutazione della conformità e dell'autorità nazionale di certificazione (di cui ai par. 1, 2 e 4 dell'art. 60 del Regolamento (UE) 2019/881), ed in conformità con le disposizioni dello specifico sistema di certificazione, comunica all'Agenzia ed all'*Ufficio unico di collegamento designato per l'Italia*[108], ogni aggiornamento in merito agli organismi di valutazione della conformità accreditati quanto a nuovi rilasci, revoche, sospensioni e limitazioni dei certificati di accreditamento per la successiva notifica da parte dell'Agenzia alla Commissione europea. L'Agenzia partecipa con propri rappresentanti alle deliberazioni dell'*Organismo di accreditamento* in ordine allo svolgimento di tali attività.

Qualora un sistema europeo di certificazione stabilisca, conformemente alle previsioni di cui dell'art. 54, par. 1, lettera f), del Regolamento (UE) 2019/881, requisiti specifici o supplementari a cui sono soggetti gli organismi di valutazione della conformità al fine di garantire che abbiano la competenza tecnica per valutare i requisiti di cibersicurezza, solo gli organismi di valutazione della conformità che soddisfano detti requisiti sono autorizzati dall'Agenzia a svolgere i compiti previsti da tale sistema.

In relazione alle attività di vigilanza nazionale e di rilascio dei certificati, l'Agenzia, con provvedimento adottato secondo la descritta procedura di cui all'art. 5, comma 3, del D.P.C.M. n. 223/2021 (cfr. *supra*), costituisce, aggiorna e rende pubblici due elenchi di esperti e di laboratori di prova da essa abilitati ad operare rispettivamente a supporto delle attività di vigilanza e rilascio dei certificati in capo all'Agenzia. Gli esperti e i laboratori di prova inseriti nell'elenco dei soggetti abilitati, iscritti nell'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale (di cui all'art. 5, comma 7 del D.Lgs. 123/2022), non possono effettuare attività di valutazione per l'emissione di certificati con livello di affidabilità *sostanziale* o *di base* in ambito nazionale, né possono essere accreditati come organismi di valutazione della conformità per il rilascio di tali certificati. Con la medesima procedura testé richiamata, sono individuate le modalità per l'abilitazione e l'eventuale rinnovo, l'inserimento, la sospensione e la cancellazione di esperti e laboratori di prova dai suddetti elenchi.

Gli oneri derivanti dall'abilitazione, le spese per le eventuali attività di autorizzazione e gli eventuali successivi aggiornamenti, conformemente all'art. 30, commi 4 e 5, della L. 24

[108] Ai sensi dell'art. 10, par. 3, del Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, *sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011*, ogni Stato membro designa un ufficio unico di collegamento. La designazione, quindi avviene ad opera dello stesso Stato membro.

dicembre 2012, n. 234[109],sono a carico dell'esperto o dell'organismo di valutazione della conformità richiedente l'abilitazione o l'autorizzazione.

7. L'attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della *cybersicurezza*

L'agenzia può realizzare progetti di ricerca al fine di elevare il livello nazionale di *cybersicurezza*. Rientrano in quest'ambito anche i progetti per lo sviluppo di *software* e di formazione, anche in collaborazione con università, centri di ricerca o laboratori specializzati nel campo della valutazione della sicurezza informatica, anche nel contesto di attività di supporto alla standardizzazione a livello nazionale, europeo ed internazionale (art. 9).

L'Agenzia monitora gli sviluppi nel campo della certificazione della *cybersicurezza*, anche consultando i portatori di interesse nazionale del settore e scambiando informazioni, esperienze e buone pratiche con la Commissione europea e le altre autorità nazionali della *cybersicurezza*.

Conformemente all'articolo 57 del Regolamento (UE) 2019/881 ed in assenza di un sistema europeo di certificazione, *l'Agenzia può introdurre sistemi di certificazione nazionali della cybersicurezza, per prodotti TIC, servizi TIC o processi TIC.*

8. Il sistema sanzionatorio

L'art. 10 prevede che l'Agenzia, in caso di violazione degli obblighi del quadro europeo di certificazione della cybersicurezza, irroghi sanzioni pecuniarie ed accessorie, chiedendo la cessazione immediata della violazione. Si applica, in quanto compatibile, la disciplina generale in materia di sanzioni amministrative di cui alla legge 24 novembre 1981, n. 689[110].

L'art. 10 contiene una lunga elencazione di fattispecie per le quali individua, nel minimo e nel massimo la sanzione amministrativa applicabile. Nello specifico, salvo che il fatto costituisca reato:

---

[109] In particolare, i commi 4 e 5, dell'art. 30, L. 24 dicembre 2012, n. 234 *Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea* prevedono che:
[...]
4. Gli oneri relativi a prestazioni e a controlli da eseguire da parte di uffici pubblici, ai fini dell'attuazione delle disposizioni dell'Unione europea di cui alla legge di delegazione europea per l'anno di riferimento e alla legge europea per l'anno di riferimento, sono posti a carico dei soggetti interessati, ove ciò non risulti in contrasto con la disciplina dell'Unione europea, secondo tariffe determinate sulla base del costo effettivo del servizio reso. Le tariffe di cui al primo periodo sono predeterminate e pubbliche.
5. Le entrate derivanti dalle tariffe determinate ai sensi del comma 4 sono attribuite, nei limiti previsti dalla legislazione vigente, alle amministrazioni che effettuano le prestazioni e i controlli, mediante riassegnazione ai sensi del regolamento di cui al decreto del Presidente della Repubblica 10 novembre 1999, n. 469.

[110] L'esercizio di tale potere sanzionatorio si pone in linea di coerenza con le previsioni di cui all'art. 7, comma 1, lett. e), del D.L. n. 82/2021, alla luce del quale l'Autorità nazionale di certificazione della *cybersicurezza* assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni.

a) l'organismo di valutazione della conformità che emette un certificato di cybersicurezza non conforme è punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. In caso di omessa revoca di un certificato da parte dell'organismo su richiesta dell'Agenzia, si applica la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro;

b) il fabbricante o fornitore che emette una dichiarazione UE di conformità volontaria non conforme è punito con la sanzione del pagamento di una somma da 15.000 euro a 75.000 euro. In caso di omessa revisione o revoca di dichiarazione UE di conformità volontaria o obbligatoria ai sensi dell'articolo 7, comma 3, si applica la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro;

c) in caso di obbligatorietà di una dichiarazione UE di conformità o di un certificato di *cybersicurezza*, il fabbricante o fornitore che mette a disposizione sul mercato un prodotto TIC o servizio TIC privo di dichiarazione UE di conformità obbligatoria o con dichiarazione UE di conformità obbligatoria non conforme o in assenza del certificato di cybersicurezza obbligatorio, è punito con la sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato il fabbricante o fornitore che per la messa a disposizione sul mercato di un prodotto TIC o di un servizio TIC si avvale di un processo TIC privo di dichiarazione UE di conformità obbligatoria o con dichiarazione UE di conformità obbligatoria non conforme o in assenza di certificato di *cybersicurezza* obbligatorio. Inoltre, l'Agenzia dispone il ritiro del prodotto o l'inibizione del servizio dal mercato a carico esclusivo del fabbricante o del fornitore indicando i tempi ed eventuali modalità per il richiamo dei prodotti già immessi sul mercato o per l'inibizione del servizio. Il fornitore che non ottempera a quanto prescritto per l'inibizione del servizio dal mercato è assoggettato alla sanzione amministrativa da 60.000 euro a 300.000 euro;

d) il fabbricante che non ottempera a quanto prescritto per il richiamo di prodotti già immessi sul mercato è assoggettato alla sanzione del pagamento di una somma da 60.000 euro a 300.000 euro. Nel caso in cui il fabbricante non ottemperi al richiamo di prodotti dal mercato, l'Agenzia, trascorsi sei mesi dalla scadenza fissata, può provvedere, al sequestro dei prodotti in questione dal mercato, a spese del fabbricante;

e) il titolare di un certificato europeo di *cybersicurezza* che non notifichi eventuali vulnerabilità o irregolarità rilevate in relazione alla sicurezza dei prodotti TIC, servizi TIC o processi TIC certificati è punito con la sanzione del pagamento di una somma da 60.000 euro a 300.000 euro. Alla medesima sanzione è assoggettato l'organismo di valutazione della conformità emittente un certificato di *cybersicurezza* o il suo titolare ovvero il fornitore o fabbricante emittente una dichiarazione UE di conformità, che

dovesse rilevare o venire a conoscenza della presenza di vulnerabilità nel prodotto TIC, servizio TIC o processo TIC certificato o dichiarato conforme, che non siano state riscontrate durante il processo di valutazione, e non ottemperi agli obblighi riguardanti il modo in cui segnalare e trattare le vulnerabilità previste per lo specifico sistema di certificazione;

f) il fabbricante o fornitore che non renda disponibile, per il periodo stabilito la dichiarazione UE di conformità o la documentazione tecnica o tutte le altre informazioni pertinenti o non trasmetta una copia della dichiarazione UE di conformità all'Agenzia o ad ENISA, ovvero non renda disponibili pubblicamente una o più delle informazioni previste ai sensi dell'art. 55 del Regolamento (UE) 2019/881[111] o non rispetti il formato o le procedure di aggiornamento delle stesse informazioni o pubblichi informazioni non corrette sui certificati detenuti o sulle dichiarazioni UE di conformità emesse, è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato il fornitore o fabbricante che non comunichi la revisione o la revoca di una dichiarazione UE di conformità;

g) l'organismo di valutazione della conformità che non ottempera agli obblighi di divulgazione dei certificati europei di *cybersicurezza* rilasciati, modificati o revocati come previsto nell'ambito dello specifico sistema di certificazione è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro. Alla medesima sanzione è assoggettato l'organismo di valutazione della conformità autorizzato dall'Agenzia che non specifichi nella procedura per i reclami l'inoltro degli stessi per conoscenza anche all'Agenzia;

h) nel caso di accertamento di esercizio di organismo di valutazione della conformità senza autorizzazione si applica la sanzione del pagamento di una somma da 120.000

---

[111] Si riporta, per completezza l'art. 55 del Regolamento (UE) 2019/881:

Informazioni supplementari sulla cibersicurezza dei prodotti TIC, servizi TIC e processi TIC certificati

1. Il fabbricante o fornitore di prodotti TIC, servizi TIC o processi TIC certificati o prodotti TIC, servizi TIC o processi per i quali è stata rilasciata una dichiarazione UE di conformità rende pubblicamente disponibili le seguenti informazioni supplementari sulla cibersicurezza:

a) orientamenti e raccomandazioni che assistano gli utenti finali nel configurare, installare, avviare, operare e mantenere in modo sicuro i prodotti TIC o servizi TIC;

b) il periodo durante il quale agli utenti finali sarà offerta assistenza di sicurezza, in particolare per quanto concerne la disponibilità di aggiornamenti connessi alla cibersicurezza;

c) informazioni di contatto del fabbricante o fornitore e metodi accettati per ricevere informazioni sulle vulnerabilità dagli utenti finali e dai ricercatori nel settore della sicurezza;

d) un riferimento ad archivi online in cui siano elencate le vulnerabilità comunicate al pubblico relative al prodotto TIC, servizio TIC o processo TIC e a tutti i relativi consigli in materia di cibersicurezza.

2. Le informazioni di cui al paragrafo 1 sono disponibili in formato elettronico, restano disponibili e sono aggiornate, ove necessario, almeno fino alla scadenza del certificato europeo di cibersicurezza o della dichiarazione UE di conformità corrispondenti.

euro a 600.000 euro e al soggetto non possono essere rilasciate ulteriori autorizzazioni nei successivi tre anni dall'accertamento della violazione. Se l'autorizzazione è scaduta da meno di un anno la sanzione è compresa tra 30.000 euro e 150.000 euro ed il soggetto può richiedere il rilascio di nuova autorizzazione;

i) il richiedente di una certificazione che nell'ambito dello svolgimento dell'attività di valutazione e di rilascio dei certificati, scientemente, fornisce dati, informazioni o documentazione falsi o ometta informazioni necessarie per espletare la certificazione è assoggettato alla sanzione del pagamento di una somma da 90.000 euro a 450.000 euro. Alla medesima sanzione è assoggettato il soggetto che, scientemente, durante le verifiche di vigilanza, a cui è sottoposto fornisce dati, informazioni o documentazione falsi;

l) il fabbricante che viola le condizioni di utilizzo degli eventuali marchi o etichette previste da un sistema europeo di certificazione è assoggettato alla sanzione del pagamento di una somma da 30.000 euro a 150.000 euro;

m) l'organismo di valutazione della conformità che non ottempera agli eventuali obblighi riguardanti la conservazione dei registri è assoggettato alla sanzione del pagamento di una somma da 45.000 euro a 225.000 euro.

Nel caso in cui, in esito ad un accertamento di non conformità, sia revocato o decada un certificato obbligatorio per la messa a disposizione sul mercato di un prodotto TIC o di un servizio TIC, l'Agenzia dispone il ritiro del prodotto o l'inibizione del servizio dal mercato a carico esclusivo del fabbricante o del fornitore indicando i tempi ed eventuali modalità per il richiamo dei prodotti già immessi sul mercato o per l'inibizione del servizio; il fornitore che non ottempera a quanto prescritto per l'inibizione del servizio dal mercato è assoggettato alla sanzione amministrativa da 60.000 euro a 300.000 euro.

L'Agenzia, ai sensi del comma 15, dell'art. 10 del D.Lgs. n. 123/2022, può impartire ordini o intimare diffide ai soggetti che operano in contrasto con quanto previsto dal quadro europeo di certificazione. Ai soggetti che non ottemperano nel termine indicato nell'ordine o nella diffida l'Agenzia commina la sanzione del pagamento di una somma da 200.000 euro ad 1.000.000 di euro. Se le violazioni riguardano provvedimenti adottati dall'Agenzia nei confronti di soggetti con fatturato pari almeno a 200.000.000 euro[112], si applica a ciascun soggetto interessato una sanzione amministrativa pecuniaria non inferiore allo 0,3 per cento e

[112] Come riferimento per il fatturato si assume il valore realizzato dallo stesso soggetto nell'esercizio precedente a quello in cui sia stato impartito l'ordine o sia stata intimata la diffida.

non superiore all'1,5 per cento del fatturato, restando comunque fermo il limite massimo di 5.000.000 di euro.
I valori minimi e massimi di queste sanzioni pecuniarie sono triplicati, se la violazione ha riguardato un certificato relativo ad un prodotto TIC, ad un servizio TIC o ad un processo TIC rilasciato nell'ambito di un sistema di certificazione destinato all'utilizzo con le finalità o nell'ambito di un servizio essenziale o di un servizio di comunicazione elettronica. Resta, comunque fermo il limite di 5.000.000 di euro come sanzione massima applicabile.
Con un provvedimento dell'Agenzia (adottato secondo la procedura di cui all'art. 5, comma 3, del D.P.C.M. 9 dicembre 2021, n. 223) sono definiti i criteri di graduazione nell'irrogazione delle sanzioni pecuniarie[113].

L'autorizzazione di un organismo di valutazione della conformità ad operare nel sistema europeo di certificazione, ove prevista, è sospesa per 6 mesi o revocata nel caso di più di due violazioni del quadro europeo di certificazione rispettivamente in un quinquennio o in un biennio. In caso di revoca dell'autorizzazione, il trasgressore non può ottenere nuova autorizzazione nei successivi cinque anni dal provvedimento di revoca.

9. I Reclami sui certificati di cybersicurezza e sulle dichiarazioni UE di conformità e il Ricorso all'autorità giudiziaria

Le persone fisiche e giuridiche, ai sensi dell'art. 11 del D.L. 123/2022, hanno il diritto di presentare un reclamo all'emittente di un certificato europeo di *cybersicurezza* o all'Agenzia se il reclamo riguarda un certificato europeo di *cybersicurezza* rilasciato dall'organismo di certificazione dell'Agenzia o da suo organismo di valutazione della conformità che agisce in conformità della normativa eurounitaria.
Avverso le decisioni degli organismi di valutazione della conformità diversi dall'organismo di certificazione può essere proposta procedura di reclamo a tal fine indicata dagli stessi organismi. Nel caso in cui i sistemi europei di certificazione della cibersicurezza stabiliscano requisiti specifici o supplementari per l'autorizzazione a svolgere i compiti da essi previsti, la procedura di reclamo indicata dall'organismo prevede l'inoltro del reclamo da parte del reclamante oltreché all'organismo anche per conoscenza all'Agenzia.

[113] Nelle more dell'adozione del provvedimento in questione per la definizione dei criteri di graduazione si applicano i criteri di cui all'articolo 11 della legge 24 novembre 1981, n. 689, il quale dispone che *Nella determinazione della sanzione amministrativa pecuniaria fissata dalla legge tra un limite minimo ed un limite massimo e nell'applicazione delle sanzioni accessorie facoltative, si ha riguardo alla gravità della violazione, all'opera svolta dall'agente per la eliminazione o attenuazione delle conseguenze della violazione, nonché alla personalità dello stesso e alle sue condizioni economiche.*

Avverso le decisioni dell'Agenzia riguardanti le certificazioni oppure le dichiarazioni UE di conformità rilasciate a seguito del processo di autovalutazione (ove consentito) i sensi dell'art. 53 del Regolamento (UE) 2019/881, può essere proposta procedura di reclamo. Il reclamante formula istanza all'Agenzia, identificando il certificato di *cybersicurezza* o la dichiarazione UE di conformità oggetto del reclamo, le ragioni del reclamo e le azioni correttive che ritiene necessarie.

L'Agenzia, a seguito tale tipologia di reclamo, informa il reclamante dello stato del procedimento e della decisione adottata e informa il reclamante del diritto a un ricorso giurisdizionale effettivo. L'Agenzia risponde ai reclami entro novanta giorni dal ricevimento dell'istanza. In caso di mancata risposta ad un reclamo inoltrato all'Agenzia entro i termini previsti, il reclamo si intende rigettato (c.d. *silenzio-rifiuto*).

Il successivo art. 12 riconosce a persone fisiche e giuridiche il diritto di impugnazione avverso:

a) le decisioni assunte dall'Agenzia o dagli organismi di valutazione della conformità, anche, se del caso, in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di *cybersicurezza* detenuto da tali persone fisiche e giuridiche;
b) il mancato o parziale accoglimento di un reclamo presentato all'Agenzia o agli organismi di valutazione della conformit.

9.1 Il Ricorso all'autorità giudiziaria

Il successivo art. 12 chiarisce che fatti salvi eventuali ricorsi amministrativi o altri ricorsi di tipo extragiudiziale, le persone fisiche e giuridiche possono proporre impugnazione avverso:

a) le decisioni assunte dall'Agenzia o dagli organismi di valutazione della conformità, anche, se del caso, in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di cybersicurezza detenuto da tali persone fisiche e giuridiche;
b) il mancato o parziale accoglimento di un reclamo presentato all'Agenzia o agli organismi di valutazione della conformità.

Il secondo comma del citato art. 12 chiarisce come tali impugnazioni siano devolute alla cognizione del giudice amministrativo. In particolare, i ricorsi contro le decisioni dell'Agenzia sono presentati dinanzi al tribunale amministrativo regionale del Lazio, mentre quelli contro le decisioni degli altri organismi di valutazione della conformità al tribunale amministrativo del luogo ove è ubicata la sede di tali organismi.

10. La Destinazione dei proventi derivanti dalle attività dell'Agenzia

Le attività di vigilanza, certificazione, autorizzazione, e abilitazione sono sottoposte a tariffa, da calcolarsi sulla base dei costi effettivi dei servizi resi[114] (art. 13, D.Lgs. n. 123/2022). Le tariffe e le modalità di riscossione sono determinate con decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, su proposta del Direttore generale dell'Agenzia. Tale decreto dispone, altresì, sulle modalità di calcolo delle spese per l'impiego di esperti o laboratori abilitati dall'Agenzia per le attività di vigilanza.

Gli introiti derivanti dalle sanzioni pecuniarie sono versati in un apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati con decreto del Ministro dell'economia e delle finanze sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione dei capitoli del bilancio dell'Agenzia destinati alle attività di ricerca e formazione concernenti la certificazione della *cybersicurezza* di prodotti TIC, servizi TIC e processi TIC.

Le spese sostenute dall'Agenzia per l'adeguamento dei sistemi informativi sono coerenti con il *Piano triennale per l'informatica nella pubblica amministrazione* ai sensi dei commi da 512 a 520, dell'art. 1 della L. 28 dicembre 2015, n. 208 (art. 14).

Dall'attuazione del D.Lgs. n. 123/2022, ad esclusione dell'articolo 4, comma 3 (cfr. *supra*), non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e l'Agenzia provvede con le risorse umane, strumentali e finanziarie previste a legislazione vigente.

Il Ministro dell'economia e delle finanze è autorizzato, dal quarto comma dell'art. 14, ad apportare le occorrenti variazioni di bilancio negli stati di previsione interessati.

[114] I relativi proventi sono versati su di un apposito capitolo dell'entrata del bilancio dello Stato per essere successivamente riassegnati, con decreto del Ministro dell'economia e delle finanze, sul pertinente capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione degli appositi capitoli dell'Agenzia.