MISSIONE 1 – COMPONENTE 1 – La Cybersicurezza nella normativa italiana ed europea

PNRR

Dossier

Sommario

La Cybersicurezza nella normativa italiana: il Decreto-legge 14 giugno 2021, n. 82 2

La Cybersicurezza nella normativa europea: il D.Lgs. 3 agosto 2022, n. 123 e l'attuazione del quadro per l'introduzione di sistemi europei di certificazione 18

La Cybersicurezza nella normativa italiana: il Decreto-legge 14 giugno 2021, n. 82

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*.[1]

Tale normativa ha rimodellato l'architettura istituzionale di cybersicurezza, riorganizzando ruoli e responsabilità specifiche e il quadro normativo di riferimento, ponendo al centro della nuova governance l'Agenzia per la cybersicurezza nazionale.

La straordinaria necessità e urgenza sottesa all'introduzione del decreto-legge in analisi, dettata dal numero esponenziale di attacchi e incidenti di cybersicurezza, è connessa all'attuazione del PNRR, in cui la sicurezza dello spazio cibernetico è cruciale per garantire l'effettiva ripresa sociale ed economica del Paese, costituendone l'innesco principale. Tale cornice normativa è necessaria anche per garantire la resilienza cibernetica nazionale ponendo le condizioni necessarie per l'efficace realizzazione della ripresa nazionale, strettamente correlata allo sviluppo di capacità e competenze adeguate atte a garantire la sicurezza dello spazio cibernetico.

Il sistema di governance della cybersicurezza

La normativa in analisi delinea una nuova cornice di governance istituzionale definendo il quadro normativo nazionale in materia di cybersicurezza, introducendo una nuova agenzia pubblica specializzata, in linea con Francia e Germania, vocata alla costruzione e allo sviluppo di capacità nazionali di resilienza cibernetica.[2] L'istituzione dell'Agenzia per la cybersicurezza nazionale con la connessa cristallizzazione di specifiche attribuzioni, sinergie e responsabilità per i vari attori istituzionali coinvolti consentono di tratteggiare il quadro di governance nazionale teso a dare effettiva applicazione del quadro normativo nazionale in materia di cybersicurezza.

[1] L'adozione del D.L. 14 giugno 2021, n. 82 ha ridefinito l'architettura nazionale cyber e istituito l'Agenzia per la Cybersicurezza Nazionale (ACN) a tutela degli interessi nazionali nel campo della cybersicurezza.
[2] Per approfondimenti: Desidera, Curingia, Ferrari, Rivista Privacy& n.3 ottobre 2021

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 cybersecurity, 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 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. In particolare, 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 in materia di cybersicurezza. La ridefinizione dell'architettura istituzionale di cybersicurezza, contenuta nel decreto-legge, 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)[3]. 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 Consiglio dei ministri e il *Comitato interministeriale per la cybersicurezza* (CIC)[4]. 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*:

[3] Rivista Privacy& n.3 ottobre 2021

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* (CIC);

c) la nomina e la revoca del direttore generale e del vicedirettore generale dell'*Agenzia per la cybersicurezza nazionale*[5], previa deliberazione del Consiglio dei ministri[6].

Ai fini dell'esercizio delle competenze relative all'alta direzione delle politiche di *cybersicurezza*, il Presidente del Consiglio dei ministri, sentito il CIC, 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 delegare all'*Autorità delegata* di cui all'art. 3 della legge 3 agosto 2007, n. 124[7]. Ove sia istituita detta Autorità, le funzioni, in materia di *cybersicurezza,* non possono essere attribuitegli in via esclusiva.

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

[5] L'ACN è l'Autorità nazionale per la cybersicurezza e garantisce il coordinamento tra i soggetti pubblici coinvolti nella materia attraverso una struttura che persegue l'eccellenza, dal reclutamento alla formazione continua del personale, al fine di creare e mantenere in Italia quelle competenze – allo stato dell'arte internazionale – necessarie per guidare il Paese nel complesso processo multidimensionale di innalzamento continuo della resilienza cibernetica nazionale. Per questo l'ACN promuove la realizzazione di azioni comuni volte a garantire la sicurezza e la resilienza cibernetica necessarie allo sviluppo digitale del Paese. Persegue, inolotre, il conseguimento dell'autonomia strategica nazionale ed europea nel settore del digitale, in sinergia con il sistema produttivo nazionale, nonché attraverso il coinvolgimento del mondo dell'università e della ricerca. Favorisce, poi, specifici percorsi formativi per lo sviluppo della forza lavoro nel settore e sostiene campagne di sensibilizzazione, oltre che una diffusa cultura della cybersicurezza. Promuove, infine, la cooperazione e lo sviluppo di azioni e progetti internazionali volti alla realizzazione di un cyberspazio globale sicuro. (Fonte https://www.acn.gov.it/)

[6] Il Presidente del Consiglio dei ministri informa preventivamente il *Comitato parlamentare per la sicurezza della Repubblica* (COPASIR) e le Commissioni parlamentari competenti circa le nomine del direttore generale e del vicedirettore generale dell'*Agenzia per la cybersicurezza nazionale*.

[7] Ai sensi dell'art. 3 della Legge 3 agosto 2007, n. 124 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 dal Presidente del Consiglio dei ministri a norma della L. n. 124/2007 e in materia di *cybersicurezza* (ad eccezione delle funzioni attribuite al Sottosegretario di Stato alla Presidenza del Consiglio dei ministri, con funzioni di Segretario del Consiglio medesimo). Il Presidente del Consiglio dei ministri è costantemente informato dall'Autorità delegata sulle 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.

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*[8].

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 Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto, oltre all'Autorità delegata, ove istituita:

- dal Ministro degli affari esteri e della cooperazione internazionale;
- dal Ministro dell'interno;
- dal Ministro della giustizia;
- dal Ministro della difesa;

[8] I primi quattro articoli del decreto intervengono sul Sistema Nazionale di Sicurezza Cibernetica (SNSC), articolazione istituzionale che trova origine nel D.P.C.M. n. 66 del 19 marzo 2013 (Decreto Monti), successivamente modificato con il D.P.C.M. n. 87 del 17 febbraio 2017 (decreto Gentiloni), ove si organizzava un'architettura sviluppata su tre livelli. Si precisa che il previgente sistema di cybersicurezza nazionale, istituito con il Decreto Monti, D.P.C.M. n. 66 del 19 marzo 2013, e poi modificato con il Decreto Gentiloni, D.P.C.M. n. 87 del 17 febbraio 2017 , prevedeva altri organi deputati alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali, indicando a tal fine i compiti affidati a ciascuna componente ed i meccanismi e le procedure da seguire ai fini della riduzione della vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni e del ripristino immediato della funzionalità dei sistemi in caso di crisi. Questi erano rispettivamente: l'Organismo di supporto al CISR, il Comitato scientifico e il NISP - Tavolo interministeriale di crisi cibernetica (i quali non vennero riconfermati come componenti del sistema nel Decreto Gentiloni), e infine, gli operatori privati «che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici» (di cui all'art. 11). Per approfondimenti, vedi l'articolo "La nuova architettura di cybersicurezza nazionale: note a prima lettura del Decreto-legge n. 82 del 2021", pubblicato in federalismi.it

- dal Ministro dell'economia e delle finanze;
- dal Ministro dello sviluppo economico;
- dal Ministro della transizione ecologica;
- dal Ministro dell'università e della ricerca;
- dal Ministro delegato per l'innovazione tecnologica e la transizione digitale;
- dal Ministro delle infrastrutture e della mobilità sostenibili.

Il direttore generale dell'*Agenzia per la cybersicurezza nazionale* svolge le funzioni di segretario del Comitato.[9]

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.

Il sesto comma dell'art. 4 del D.L. n. 82/2021 chiarisce che il Comitato svolge altresì le funzioni già attribuite al *Comitato interministeriale per la sicurezza della Repubblica* (CISR)[10], dal c.d.

9 In una comparazione diacronica tra compagini istituzionali è possibile considerare che l'articolazione di natura politica, vedeva il Presidente del Consiglio dei ministri posto al vertice del sistema, supportato dal Comitato Interministeriale per la sicurezza della Repubblica (CISR), quale organo istituito con Legge 3 agosto 2007, n. 124 presso la Presidenza del Consiglio dei Ministri, e avente funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza. Il secondo livello, di carattere operativo e amministrativo, vedeva la partecipazione del Nucleo per la Sicurezza Cibernetica (NSC), istituito nell'ambito dell'Ufficio del Consigliere Militare presso la Presidenza del Consiglio dei ministri, con la funzione di supportare il Presidente nella materia della sicurezza del "cyberspazio" per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. Il terzo livello era invece composto dagli Organismi di informazione per la sicurezza, responsabili di condurre attività di ricerca informativa, nonché analisi, valutazioni e previsioni sulle minacce, ed alla trasmissione di informazioni rilevanti al Nucleo per la Sicurezza Cibernetica, e agli altri soggetti – sia pubblici che privati – interessati all'acquisizione di informazioni. In considerazione di ciò, preme innanzitutto osservare che, diversamente dalla precedente organizzazione, con il Decreto-legge n. 82/2021 si è inteso creare un'organizzazione non più afferente al Sistema di informazione per la sicurezza della Repubblica, ma un modello organizzativo separato e specializzato nel particolare settore della "sicurezza nel cyberspazio". Ne sono prova l'introduzione di due organi ad hoc, quali, il Comitato Interministeriale per la Cybersicurezza (CIC), l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN), nonché la mancata conferma degli Organismi di informazione per la sicurezza tra gli attori componenti il nuovo SNSC. La nuova architettura, incardinata nella Presidenza del Consiglio dei ministri, continua ad essere legata alla medesima direzione operativa e strategica del Sistema di informazione per la sicurezza della Repubblica di cui alla L 3 agosto 2007, n. 124. Nel primo livello l'attuale SNSC affida, infatti, al Presidente del Consiglio dei ministri – ovviamente confermandone la posizione di vertice del Sistema – compiti più estesi ed elevati rispetto a quelli assegnati nella previgente architettura. In particolare, richiamando la formulazione dell'art. 1 dell'appena citata L. n. 124 del 2007, l'art. 1, co. 1, lett. a) del decreto attribuisce in via esclusiva al Presidente «l'alta direzione e la responsabilità generale delle politiche di cybersicurezza, anche ai fini della sicurezza nazionale nel cyberspazio». Le ulteriori attribuzioni, di cui alle lett. b) e c) del medesimo disposto, interessano invece l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato Interministeriale per la Cybersicurezza (CIC), nonché la nomina e la revoca del direttore generale e del vicedirettore generale dell'Agenzia per la Cybersicurezza Nazionale (ACN), previa deliberazione del Consiglio dei ministri, e, ai sensi dell'art. 1, co. 3 del decreto, informando preventivamente di tali nomine il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), e le Commissioni parlamentari competenti. Si tratta di un documento la cui stesura è contemplata all'art. 7 della direttiva NIS, rubricato "Strategia nazionale in materia di sicurezza della rete e dei sistemi informativi". Per approfondimenti, vedi l'articolo "La nuova architettura di cybersicurezza nazionale: note a prima lettura del Decreto-legge n. 82 del 2021", pubblicato in federalismi.it

10 Di cui all'art. 5 della Legge 3 agosto 2007, n. 124.

Decreto-legge perimetro[11] 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.

Come evidenziato in letteratura è opportuno rilevare lo sforzo del legislatore nella ricerca di un punto di equilibrio teso a garantire, da un lato, l'attribuzione di un'autonoma personalità giuridica all'Agenzia (che esercita le funzioni che le sono attribuite dal decreto tramite i propri organi e, in particolare, tramite il direttore generale che ne è anche legale rappresentante) la cui attività è incardinata, dall'altro lato, in un alveo di regole definito dal decreto-legge istitutivo e, di riflesso, posta in attuazione di quanto previsto dai regolamenti e dalle direttive impartite dal Presidente del Consiglio dei ministri e dall'Autorità delegata (per i poteri a questa demandati), che possono avvalersi dell'Agenzia per l'esercizio delle competenze a essi attribuite dal decreto-legge in parola.

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.

[11] 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*.

Gli incarichi del direttore generale e del vicedirettore generale hanno la durata massima di quattro anni e sono rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni[12].

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[13].

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[14], entro centoventi giorni dalla data di entrata in vigore della Legge di conversione del D.L. 82/2021[15].

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 vicedirettore generale dell'Agenzia;

b) la composizione e il funzionamento del Collegio dei revisori dei conti;

c) l'istituzione di eventuali sedi secondarie.

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[16], il

[12] Il direttore generale ed il vicedirettore generale, ove provenienti da pubbliche amministrazioni sono collocati fuori ruolo o in posizione di comando o altra analoga posizione, secondo gli ordinamenti di appartenenza.
[13] 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.
[14] 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.
[15] 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.
[16] 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*.

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*;

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[17], 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);

[17] 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.

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[18] 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 definizione delle caratteristiche di qualità, sicurezza, *performance* e scalabilità, interoperabilità, portabilità dei servizi *cloud* per la pubblica 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*;

[18] Con particolare riferimento al potere di adottare linee guida contenenti regole tecniche di *cybersicurezza* ai sensi dell'articolo 71 del CAD.

q) coordina, in raccordo con il *Ministero degli affari esteri e della cooperazione internazionale*, la cooperazione internazionale nella materia della *cybersicurezza*[19];

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 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;

[19] 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;

v-bis) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni[20];

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.

Presso l'Agenzia, anche ai fini dell'esercizio delle funzioni sub r), s), t), u), v), z) e aa), presso l'Agenzia 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[21]. 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 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, per le finalità di cui al presente decreto, consulta il 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.

[20] In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile.
[21] Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.

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.

Detto nucleo è presieduto dal Direttore Generale dell'Agenzia o, per sua delega, dal Vicedirettore Generale ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, dell'Agenzia informazioni e sicurezza esterna (AISE), dell'Agenzia informazioni e sicurezza interna (AISI), di ciascuno dei Ministeri rappresentati nel CIC e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri[22]. I componenti del Nucleo possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della *cybersicurezza*. Ai componenti del Nucleo non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

Nell'ambito della *mission* istituzionale il Nucleo per la *cybersicurezza* svolge, ai sensi dell'art. 9, D.L. 82/2021, i seguenti compiti:

a) può formulare proposte di iniziative in materia di *cybersicurezza* del Paese, anche nel quadro del contesto internazionale in materia;

b) promuove la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile;

c) promuove e coordina lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale a esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

d) valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della *cybersicurezza*, procedure di condivisione delle informazioni, anche con gli

[22] Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124 del 2007.

operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi;

e) acquisisce, anche per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi dagli organismi di informazione, dalle Forze di polizia e, in particolare, dall'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, dalle strutture del Ministero della difesa, nonché dalle altre amministrazioni che compongono il Nucleo e dai gruppi di intervento per le emergenze informatiche (*Computer Emergency Response Team* - CERT) istituiti ai sensi della normativa vigente;

f) riceve dal CSIRT Italia le notifiche di incidente ai sensi delle disposizioni vigenti;

g) valuta se gli eventi sub e) e f) assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale, provvedendo in tal caso a informare tempestivamente il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita.

La Gestione delle crisi che coinvolgono aspetti di cybersicurezza

Ai sensi dell'art. 10 del D.L. 82/2021 nelle situazioni di crisi che coinvolgono aspetti di *cybersicurezza*, nei casi in cui il Presidente del Consiglio dei ministri convochi il CISR in materia di gestione di tali situazioni di crisi, alle sedute del Comitato sono chiamati a partecipare il (ministro) *delegato per l'innovazione tecnologica e la transizione digitale* e il *Direttore generale dell'Agenzia*.

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, in rappresentanza anche della Commissione interministeriale tecnica di difesa civile, autorizzati ad assumere decisioni che impegnano la propria amministrazione. Alle riunioni i componenti possono farsi accompagnare da altri funzionari della propria amministrazione. Alle stesse riunioni possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, e di altri soggetti pubblici o privati eventualmente

interessati. Per la partecipazione non sono previsti compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

È compito del Nucleo, nella composizione allargata per la gestione delle crisi, assicurare che le attività di reazione e stabilizzazione di competenza delle diverse amministrazioni ed enti rispetto a situazioni di crisi di natura cibernetica vengano espletate in maniera coordinata.

Il Nucleo, per l'espletamento delle proprie funzioni e ferme restando le prerogative del *Comitato interministeriale per la sicurezza della Repubblica* per le situazioni di crisi che coinvolgano aspetti di sicurezza nazionale (secondo le previsioni di cui all'art. 7-*bis*, comma 5, del D.L. n. 174/2015):

a) mantiene costantemente informato il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla crisi in atto, predisponendo punti aggiornati di situazione;

b) assicura il coordinamento per l'attuazione a livello interministeriale delle determinazioni del Presidente del Consiglio dei ministri per il superamento della crisi;

c) raccoglie tutti i dati relativi alla crisi;

d) elabora rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati;

e) partecipa ai meccanismi europei di gestione delle crisi cibernetiche, assicurando altresì i collegamenti finalizzati alla gestione della crisi con gli omologhi organismi di altri Stati, della NATO, dell'Unione europea o di organizzazioni internazionali di cui l'Italia fa parte.

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[23] 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.

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.

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 cui al citato art.7-bis del D.L. n. 144/2005). Il personale dell'Agenzia, nello svolgimento delle

[23] 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.
[…]

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[24].

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.

[24] 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.

La Cybersicurezza nella normativa europea: il D.Lgs. 3 agosto 2022, n. 123 e l'attuazione del quadro per l'introduzione di sistemi europei di certificazione

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 cybersicurezza*, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»).

La normativa eurounitaria persegue come finalità principale quella di garantire *il buon funzionamento del mercato interno perseguendo al contempo un elevato livello di cybersicurezza, cyber resilienza 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 cybersicurezza*);

b) un *quadro per l'introduzione di sistemi europei di certificazione della cybersicurezza* al fine di garantire un livello adeguato di cybersicurezza dei prodotti TIC[25], 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 cybersicurezza 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 cybersicurezza fornendo regole comuni in materia di disponibilità, autenticità, integrità e la riservatezza dei dati processati (conservati, trattati, e trasmessi) e dei servizi offerti *on-*

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

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

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

Il D.Lgs. n. 123/2022 individua le misure necessarie per adeguare la normativa interna al *nuovo quadro europeo di certificazione della cybersicurezza*, 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'art. 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;

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.

L'Autorità nazionale di certificazione della cybersicurezza

L'art. 4 del D.Lgs. n. 123/2022 attribuisce all'*Agenzia per la cybersicurezza nazionale* di cui all'art. 5, del D.L. 14 giugno 2021, n. 82 (convertito, con modificazioni, dalla legge 4 agosto

2021, n. 109), le funzioni di *Autorità nazionale di certificazione della cybersicurezza*, nel rispetto di quanto previsto dall'art. 58, par. 1, del Regolamento (UE) 2019/881[26].

L'organizzazione e le procedure per lo svolgimento dei compiti dell'Agenzia quale *Autorità nazionale di certificazione della cybersicurezza* sono definite con provvedimento dell'Agenzia, adottato ai sensi dell'art. 5, comma 3, del *Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale* di cui al D.P.C.M. 9 dicembre 2021, n. 223, il quale attribuisce al Direttore generale, tra le altre cose, il potere di adottare, sentito il Vice direttore generale i provvedimenti necessari per il funzionamento dell'Agenzia[27].

Attraverso tale provvedimento sono definite, altresì, le modalità applicative delle seguenti attività:

- Vigilanza nazionale;
- Rilascio dei certificati di cybersicurezza;
- Dichiarazioni UE di conformità;
- Accreditamento ed autorizzazione degli organismi di valutazione della conformità ed abilitazione dei laboratori di prova ed esperti dell'Agenzia;
- Attività di ricerca, formazione e sperimentazione nazionale nell'ambito della certificazione della cybersicurezza;
- Reclami sui certificati di cybersicurezza e sulle dichiarazioni UE di conformità.

Infine, il secondo periodo del comma 2, dell'art. 4, specifica che il predetto provvedimento deve disporre anche la rigorosa separazione tra le attività dell'Agenzia relative al rilascio di certificati europei di cybersicurezza e quelle di vigilanza. Tali attività devono, quindi, essere svolte indipendentemente le une dalle altre, nell'ambito di due distinte Divisioni[28].

[26] A tal proposito si ricorda che la citata norma eurounitaria prevede che ciascuno Stato membro designi una o più autorità nazionali di certificazione della cybersicurezza nel suo territorio oppure, con l'accordo di un altro Stato membro, designi una o più autorità nazionali di certificazione della cybersicurezza stabilite in tale altro Stato membro affinché siano responsabili dei compiti di vigilanza nello Stato membro designante.
[27] Egli, a tal fine, definisce gli indirizzi dell'Agenzia e ne coordina le attività, adottando ogni iniziativa idonea al miglior espletamento delle funzioni dell'Agenzia stessa.
[28] Ai sensi all'art. 4, comma 4, del D.P.C.M. n. 223/2021 le Divisioni sono articolazioni interne istituite per la gestione di un insieme omogeneo di tematiche e macro-processi.

L'Agenzia partecipa, con proprio personale, alle attività internazionali del *Gruppo europeo di certificazione della cybersicurezza* (ECCG) conformemente gli articoli 62 e 66 del Regolamento (UE) 2019/881.

Il successivo terzo comma autorizza la spesa di 657.500 euro per l'anno 2022, 592.500 euro per l'anno 2023 e 637.500 euro annui a decorrere dall'anno 2024 per lo svolgimento dei compiti attribuiti all'Agenzia, inerenti:

- la realizzazione e la gestione dei sistemi informativi;
- la formazione del personale tecnico ed amministrativo;
- la ricerca e l'innovazione;
- la realizzazione e l'aggiornamento di laboratori interni;
- l'abilitazione di laboratori di prova ed esperti;
- l'autorizzazione di organismi di valutazione della conformità;
- la vigilanza, l'accreditamento, il rinnovo e l'estensione dell'*Organismo di Certificazione della Sicurezza Informatica* (OCSI);
- le missioni nazionali ed internazionali;
- le spese generali.

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 in 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 organismi di valutazione della conformità[29]. 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. Resta,

[29] 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 all'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale.

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 cybersicurezza stabiliscono requisiti specifici o supplementari nonché quanto previsto dalle disposizioni in materia di funzioni di monitoraggio e vigilanza sulle attività degli organismi di valutazione. 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 pubblici di valutazione della conformità di cui all'art. 56, par. 5, lett. b), del Regolamento (UE) 2019/881[30];

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[31]. L'Agenzia esegue l'attività di vigilanza anche in collaborazione con le Forze dell'ordine.

L'Agenzia, nell'attività di vigilanza affidatale, 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.

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[32], detto certificato è sottoposto a revoca:

[30] La norma in questione prevede che in casi debitamente giustificati, un sistema europeo di certificazione della cybersicurezza può prevedere che i certificati europei di cybersicurezza 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 cybersicurezza designata ai sensi dell'art. 58, par. 1, del Regolamento (UE) 2019/881, oppure un'autorità nazionale di certificazione della cybersicurezza 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'art. 60.

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

[32] 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

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 appena 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 cybersicurezza nell'ambito della propria la politica di divulgazione dei certificati europei di cybersicurezza rilasciati, modificati o revocati nell'ambito del sistema.

L'ottavo 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 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

«sostanziale». Tale classificazione è operata sulla base dei criteri previsti dal sistema europeo di certificazione della cybersicurezza. Il successivo par. 5, lett. b), derogando parzialmente i principi di cui al comma precedente prevede che, in casi debitamente giustificati, un sistema europeo di certificazione possa prevedere che i certificati europei di cybersicurezza vengano 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 cybersicurezza richieda un livello di affidabilità «*elevato*», il certificato europeo di cybersicurezza nell'ambito di tale sistema deve essere rilasciato solo da un'autorità nazionale di certificazione della cybersicurezza oppure, nei casi seguenti, da un organismo di valutazione della conformità:

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

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.

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 all'elenco dei laboratori di prova e degli esperti per le attività di vigilanza nazionale, ferme restando, per specifici sistemi di certificazione, le possibili modalità alternative di emissione dei certificati, 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 cybersicurezza 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.

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 UE di conformità 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 il caso in cui sia diversamente specificato dalla normativa interna o da quella unionale. 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. *sopra*).

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*[33], 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 cybersicurezza, 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. *sopra*), 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 ed i laboratori di prova inseriti nell'elenco dei soggetti abilitati, iscritti all'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

[33] 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.

valutazione della conformità per il rilascio di tali certificati. Con la medesima procedura appena 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 dicembre 2012, n. 234[34], sono a carico dell'esperto o dell'organismo di valutazione della conformità richiedente l'abilitazione o l'autorizzazione.

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 la formazione, anche in collaborazione con università, centri di ricerca o laboratori specializzati nel campo della valutazione della sicurezza informatica, o 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'art. 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.

---

[34] 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.

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[35].

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:

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'art. 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

[35] 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.

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[36] 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

[36] Si riporta, per completezza l'art. 55 del Regolamento (UE) 2019/881:
Informazioni supplementari sulla cybersicurezza 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 cybersicurezza:
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 cybersicurezza;
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 cybersicurezza.
2. Le informazioni di cui al par. 1 sono disponibili in formato elettronico, restano disponibili e sono aggiornate, ove necessario, almeno fino alla scadenza del certificato europeo di cybersicurezza o della dichiarazione UE di conformità corrispondenti.

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 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[37], si applica a ciascun soggetto interessato una sanzione amministrativa pecuniaria non inferiore allo 0,3 per cento e 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[38].

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.

[37] 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.
[38] Nelle more dell'adozione del provvedimento in questione per la definizione dei criteri di graduazione si applicano i criteri di cui all'art. 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*".

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 cybersicurezza 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.

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, 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 conformità.

Sono, comunque, fatti salvi eventuali ricorsi amministrativi o altri ricorsi di tipo extragiudiziale.

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.

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[39] (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 detto Ministero, 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'art. 4, comma 3 (cfr. *sopra*), 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.

[39] 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.