dossier

XIX Legislatura

3 luglio 2024

Misure per un livello comune elevato di sicurezza cibernetica nell'Unione Europea

A.G. 164

Ai sensi degli articoli 1 e 3 della legge 21 febbraio 2024, n. 15

Senato della Repubblica

Camera dei deputati

Senato della Repubblica

SERVIZIO STUDI
TEL. 06 6706-2451 - ✉ studi1@senato.it – 𝕏 @SR_Studi

Dossier n. 308

Camera dei deputati

SERVIZIO STUDI
Dipartimento Istituzioni
Tel. 06 6760-9475 - ✉ st_istituzioni@camera.it - 𝕏 @CD_istituzioni

Dipartimento Trasporti
TEL. 06 6760-2614 st_trasporti@camera.it - 𝕏@CD_trasporti

Atti del Governo n. 164

I N D I C E

PREMESSA

L'atto del Governo n. 164 reca uno schema di decreto legislativo attuativo della direttiva dell'Unione europea n. 2555 del 2022 (c.d. direttiva NIS 2) relativa a **misure per un livello comune elevato di cybersicurezza nell'Unione europea**.

Si tratta di un settore assai delicato, oggetti negli ultimi anni dell'attenzione dei legislatori di tutto il mondo, in particolare dell'Unione europea e del Parlamento italiano (vedi l'allegato al presente *dossier* su *La disciplina della sicurezza cibernetica*).

Il tema della cybersicurezza risulta decisivo anche in connessione con lo sviluppo dell'**intelligenza artificiale**, poiché i *data set* su cui i sistemi di IA poggiano richiedono elevati livelli di **integrità** e **protezione** (si rinvia al riguardo all'apposito tema di documentazione su L'intelligenza artificiale).

Lo schema di decreto legislativo, che si compone di 6 Capi e 44 articoli, dispone l'**abrogazione del D.Lgs. n. 65 del 2018** di recepimento della prima direttiva NIS, di cui la direttiva NIS 2 dispone l'abrogazione a decorrere dal 18 ottobre 2024 e di alcune disposizioni (articoli 40 e 41) del D.Lgs. n. 259 del 2003 recante "Codice delle comunicazioni elettroniche", prevedendo una fase transitoria fino all'emanazione dei provvedimenti attuativi del decreto.

La direttiva (UE) 2022/2555 (c.d. direttiva NIS 2)

A livello di Unione europea la materia della sicurezza cibernetica è stata inizialmente regolata dalla **direttiva UE) 2016/1148 del 6 luglio 2016** che reca misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. direttiva NIS - *Network and Information Security*) al fine di conseguire un "livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea". La direttiva è stata recepita nell'ordinamento italiano con il **decreto legislativo n. 65 del 18 maggio 2018** (c.d. decreto legislativo NIS), che detta la cornice legislativa interna delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS.

Le norme introdotte nel 2016 sono state aggiornate dalla **direttiva (UE) 2022/2555 del 14 dicembre 2022** (c.d. direttiva NIS 2) che sostituisce il quadro di riferimento in materia, al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cybersicurezza. L'aggiornamento della direttiva mira inoltre ad

eliminare le ampie divergenze tra gli Stati membri che hanno attuato gli obblighi in materia di sicurezza e segnalazione degli incidenti, nonché in materia di vigilanza ed esecuzione, stabiliti dalla direttiva NIS in modi significativamente diversi a livello nazionale, con un effetto potenzialmente pregiudizievole sul funzionamento del mercato interno.

In particolare, la direttiva NIS 2 stabilisce norme minime e meccanismi per la cooperazione tra le autorità competenti di ciascuno Stato membro, aggiornando l'elenco dei settori e delle attività soggetti agli obblighi in materia e prevedendo mezzi di ricorso e sanzioni per garantirne l'applicazione.

La direttiva, in particolare:

a) stabilisce obblighi per gli Stati membri di adottare una strategia nazionale per la cybersicurezza, designare autorità nazionali competenti, punti di contatto unici e CSIRT;

b) prevede che gli Stati membri stabiliscano obblighi di gestione e segnalazione dei rischi di cybersicurezza per i soggetti indicati come soggetti essenziali nell'allegato I e come soggetti importanti nell'allegato II;

c) prevede che gli Stati membri stabiliscano obblighi in materia di condivisione delle informazioni sulla cybersicurezza.

Per quanto riguarda le principali novità, la direttiva NIS 2 **amplia il campo di applicazione**, da un lato, includendovi anche la pubblica amministrazione centrale (lasciando discrezionalità agli Stati membri di inserire gli enti locali in base all'assetto istituzionale), le piccole e microimprese (solo se operano in settori chiave per la società) e, indipendentemente dalle dimensioni, fornitori di servizi di comunicazione elettroniche pubbliche e di reti di comunicazione elettronica accessibili al pubblico, e dall'altro lato, aumentando significativamente i settori di applicazione.

Inoltre, mentre ai sensi della precedente direttiva NIS la responsabilità di determinare quali soggetti soddisfacessero i criteri per essere considerati operatori di servizi essenziali spettava agli Stati membri, la nuova direttiva NIS 2 introduce la **regola della soglia di dimensione**. Ciò significa che tutti i soggetti di medie e grandi dimensioni che operano nei settori o forniscono i servizi contemplati dalla direttiva dovrebbero rientrare nel suo ambito di applicazione.

Il nuovo regime esclude dalla sua applicazione i soggetti operanti in **settori** quali la sicurezza nazionale, la pubblica sicurezza o la difesa, il contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati. Sono altresì esclusi Parlamenti e banche centrali.

Inoltre la direttiva NIS 2 prevede l'istituzione di una **rete europea delle organizzazioni di collegamento per le crisi informatiche EU-CyCLONe**, volta a sostenere la gestione coordinata degli incidenti di cybersicurezza su vasta scala.

La direttiva (UE) 2022/2555 apporta alcune modifiche al **regolamento (UE) n. 910/2014**, noto come regolamento eIDAS (*electronic IDentification Authentication and Signature*), che fornisce una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni e incrementa la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di e-business e commercio elettronico nell'Unione Europea. In particolare, tale regolamento: fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro; stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche; istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.

Ulteriori modifiche riguardano la **direttiva (UE) 2018/1972**, che istituisce il Codice europeo delle comunicazioni elettroniche.

La disposizione di delega per il recepimento

La direttiva (UE) 2022/2555 pone come termine per il suo recepimento il **17 ottobre 2024**, abroga la direttiva (UE) 2016/1148 (c.d. direttiva NIS, *Network and Information Security*)

A tal fine, la **legge 21 febbraio 2024, n. 15** (legge di delegazione europea 2022-23), oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, stabilisce, all'**articolo 3**, gli ulteriori **princìpi e criteri direttivi specifici** di delega assegnati al Governo per il suo recepimento. Si tratta di:

- individuare i **criteri** in base ai quali un **ente pubblico può essere considerato pubblica amministrazione** ai fini dell'applicazione delle disposizioni della direttiva (UE) 2022/2555 (**lettera a**): in proposito l'articolo 2 della direttiva stabilisce infatti che essa si applica ad un ente della amministrazione centrale, quale definito da ciascuno Stato membro conformemente al diritto nazionale ovvero ad un ente pubblico a livello regionale quale definito dallo Stato, ma solo se a seguito di una valutazione basata sul rischio, si ritenga che fornisca servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche, considerando anche la possibilità l'applicazione della direttiva per i comuni e le province secondo principi di gradualità, proporzionalità e adeguatezza (come previsto a seguito dell'esame alla Camera dei deputati);
- prevedere l**'esclusione dall'ambito di applicazione** delle disposizioni della nuova direttiva NIS 2 degli enti della pubblica amministrazione operanti nei settori di cui all'articolo 2, paragrafo 7, della direttiva

medesima (**lettera b**), ossia quelli che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati, ivi **compresi gli organismi di informazione per la sicurezza** ai quali si applicano le disposizioni di cui alla legge 3 agosto 2007, n. 124;

- avvalersi della facoltà prevista per gli stati membri dall'articolo 2, paragrafo 8, della direttiva, di **esentare alcuni soggetti specifici** che svolgono attività nei settori ivi indicati (sicurezza nazionale, della pubblica sicurezza, della difesa o del contrasto) o che forniscono servizi esclusivamente agli enti della pubblica amministrazione, con la precisazione che ciò avvenga mediante uno o più decreti del Presidente del Consiglio dei ministri, adottati su proposta delle competenti Amministrazioni (**lettera c**);
- confermare la **distinzione tra l'Agenzia per la cybersicurezza nazionale**[1], quale autorità nazionale competente e punto di contatto, ai sensi della direttiva (articolo 8), e le **autorità di settor**e operanti negli ambiti di cui agli allegati I e II alla medesima direttiva (**lettera d**);

Ai sensi del D.Lgs. n. 65/2018 (articolo 7), come modificato dal D.L. 82/2021, l'Agenzia per la cybersicurezza nazionale è stata designata quale autorità nazionale competente NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III[2]. Sono designate quali autorità di settore:

a) il Ministero dello sviluppo economico, per il settore infrastrutture digitali, nonché per i servizi digitali;

b) il Ministero delle infrastrutture e della mobilità sostenibili, per il settore trasporti, sottosettori aereo, ferroviario, per vie d'acqua e su strada;

c) il Ministero dell'economia e delle finanze, per il settore bancario e per il settore infrastrutture dei mercati finanziari, in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob, secondo modalità di

[1] L'Agenzia per la cybersicurezza nazionale (ACN) è stata istituita dal decreto-legge n. 82/2021 (che ha definita l'intera governance del sistema nazionale di sicurezza cibernetica) a tutela degli interessi nazionali nel campo della cibersicurezza. L'Agenzia è l'Autorità nazionale per la cybersicurezza e in quanto tale ha il coordinamento tra i soggetti pubblici coinvolti nella cibersicurezza a livello nazionale. Promuove azioni comuni dirette ad assicurare la sicurezza cibernetica, a sviluppare la digitalizzazione del sistema produttivo e delle pubbliche amministrazioni e del Paese, nonché a conseguire autonomia (nazionale ed europea) per i prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore. Essa predispone la strategia nazionale di cibersicurezza.

[2] La qualifica di "autorità competente NIS" (in origine attribuita ai singoli ministeri in base ai settori di competenza) è stata accentrata nell'Agenzia nazionale per la cybersicurezza con il D.L. 82/2021. I singoli ministeri sono designati quali autorità di settore (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali).

collaborazione e di scambio di informazioni stabilite con decreto del Ministro dell'economia e delle finanze;

d) il Ministero della salute, per l'attività di assistenza sanitaria prestata dagli operatori dipendenti o incaricati dal medesimo Ministero o convenzionati con lo stesso, e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità sanitarie territorialmente competenti, per le attività di assistenza sanitaria prestata dagli operatori autorizzati e accreditati dalle Regioni o dalle Province autonome negli ambiti territoriali di rispettiva competenza;

e) il Ministero della transizione ecologica per il settore energia, sottosettori energia elettrica, gas e petrolio;

f) il Ministero della transizione ecologica e le Regioni e le Province autonome di Trento e di Bolzano, direttamente o per il tramite delle Autorità territorialmente competenti, in merito al settore fornitura e distribuzione di acqua potabile.

- in attuazione dell'articolo 10 della direttiva NIS 2, confermare le disposizioni del citato D.Lgs. n. 65/2018 in materia di istituzione del **CSIRT Italia**, nonché ampliare quanto previsto dal medesimo decreto prevedendo la **collaborazione tra tutte le strutture pubbliche (CERT)** coinvolte in caso di eventi malevoli alla sicurezza informatica (**lettera e**);

Già attualmente, il d.lgs. 85/2018 in attuazione della direttiva NIS, dispone che presso l'Agenzia opera il CSIRT-*Computer Emergency Response Team* italiano, con un contingente di 30 persone e lo stanziamento di specifiche risorse finanziarie, al quale sono attribuite le funzioni del CERT nazionale (in precedenza presso il Ministero per lo sviluppo economico) e del CERT-PA (in precedenza presso l'Agenzia per l'Italia digitale-AGID). Il CSIRT è definito dalla direttiva 2016/1148 quale "gruppo di intervento per la sicurezza informatica in caso di incidente", che ogni Stato membro è chiamato a designare con il compito di trattare gli incidenti e i rischi secondo una procedura definita.

L'**articolo 10 della nuova direttiva NIS 2** conferma la designazione da parte di ciascuno Stato membro di uno o più CSIRT, anche all'interno di un'autorità competente. I CSIRT devono essere conformi ai requisiti stabiliti nella direttiva e sono responsabili della gestione degli incidenti conformemente a una procedura ben definita. Gli Stati membri devono provvedere affinché ogni CSIRT disponga di un'infrastruttura di informazione e comunicazione adeguata, sicura e resiliente attraverso la quale scambiare informazioni con i soggetti essenziali e importanti e con gli altri portatori di interesse pertinenti. Devono inoltre garantire la collaborazione effettiva, efficiente e sicura dei loro CSIRT nella rete di CSIRT.

- prevedere un **regime transitorio** per i soggetti già sottoposti alla disciplina del D.lgs. n. 65/2018, di recepimento della direttiva (UE) 2016/1148, ai fini della migliore applicazione delle disposizioni previste dalla direttiva NIS2; in sede referente è stata esplicitata la necessità di garantire termini congrui di adeguamento (**lettera f**);

In merito si ricorda che il D.Lgs. n. 65/2018 definisce gli obblighi in capo agli operatori dei servizi essenziali e ai fornitori dei servizi digitali con riferimento alla sicurezza della rete e dei sistemi informativi che utilizzano nel contesto dei servizi individuati dall'allegato III. Gli operatori di servizi essenziali, ai fini del provvedimento, sono i soggetti pubblici o privati, della tipologia prevista dall'elenco dell'allegato II (settori dell'energia e trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali), individuati dalle autorità competenti NIS.

- prevedere meccanismi che consentano la **registrazione dei soggetti essenziali e importanti**, di cui all'articolo 3 della direttiva (UE) 2022/2555, ai fini della comunicazione dei dati di cui al paragrafo 4 del medesimo articolo 3; a seguito dell'esame in sede referente si prevede che tra tali soggetti siano compresi quelli che gestiscono servizi connessi o strumentali alle attività oggetto delle disposizioni della medesima direttiva relative al settore della cultura (**lettera g**);
- in relazione alle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555, prevedere, in particolare, l'individuazione, attraverso l'utilizzo di strumenti flessibili atti a corrispondere al rapido sviluppo tecnologico, delle tecnologie necessarie ad assicurare l'effettiva attivazione delle misure stesse. L'autorità amministrativa individuata come responsabile di tale procedimento dovrà provvedere all'aggiornamento degli strumenti adottati (**lettera h,** introdotta in sede referente);
- introdurre le modifiche necessarie alla legislazione vigente, anche in materia penale, al fine di assicurare il recepimento nell'ordinamento nazionale delle disposizioni della direttiva NIS 2 in tema di **divulgazione coordinata delle vulnerabilità** (**lettera i**);

La direttiva NIS 2 stabilisce (articolo 12) un quadro per la divulgazione coordinata delle vulnerabilità, che consiste in un processo strutturato attraverso il quale le vulnerabilità sono segnalate al fabbricante o al fornitore dei prodotti TIC (tecnologie dell'informazione e della comunicazione) dei servizi TIC potenzialmente vulnerabili, in modo tale da consentire loro di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico.

- definire le competenze dell'Agenzia per l'Italia digitale e dell'Agenzia per la cybersicurezza nazionale in relazione alle attività previste dal regolamento (UE) n. 910/2014, noto come regolamento eIDAS (**lettera l**);
- individuare criteri oggettivi e proporzionati ai fini dell'applicazione degli obblighi informativi di cui all'articolo 23, paragrafo 2, della direttiva (UE) 2022/2555 (**lettera m,** introdotta in sede referente);
- rivedere il **sistema sanzionatorio e il sistema di vigilanza ed esecuzione** previsto dal D.Lgs. n. 65/2018 (**lettera n**), che attualmente individua i poteri di controllo dell'autorità NIS sia nei confronti degli operatori di servizi essenziali, sia dei fornitori di servizi digitali, prevedendo poteri di verifica e di ispezione (articolo 19) oltre che l'irrogazione di sanzioni amministrative nel caso di mancato adempimento degli obblighi previsti (articoli 20 e 21). In proposito, si dispone un primo specifico criterio di delega che prevede che le nuove **sanzioni** siano **effettive, proporzionate e dissuasive rispetto alla gravità della violazione** degli obblighi derivanti dalla direttiva NIS 2, "**anche in deroga ai limiti** previsti dall'articolo 32, comma 1, lettera d), della legge n. 234/2012 e alla legge n. 689/1981" ed introducendo **strumenti deflattivi del contenzioso**;

La relazione illustrativa del disegno di legge di delegazione europea (poi divenuta L. n. 115/2024) motiva la necessità di derogare ai limiti previsti dall'articolo 32 della legge n. 234 del 2012 con riferimento all'attuazione delle disposizioni della direttiva NIS 2 che contemplano anche l'applicazione di sanzioni amministrative pecuniarie che possono raggiungere nel massimo un importo di dieci milioni di euro.

Si ricorda che l'articolo 32, comma 1, lettera d), della legge n. 234/2012 definisce i limiti delle sanzioni amministrative e penali per le infrazioni alle disposizioni dei decreti legislativi di recepimento delle direttive europee previste dalla legge di delegazione europea. Per le sanzioni penali si dispone, tra le altre cose, che queste possano essere previste nei limiti, rispettivamente, dell'ammenda fino a 150.000 euro e dell'arresto, fino a tre anni, solo nei casi in cui le infrazioni ledano o espongano a pericolo interessi costituzionalmente protetti. In tali casi, prosegue la disposizione, sono previste la pena dell'ammenda alternativa all'arresto per le infrazioni che espongano a pericolo o danneggino l'interesse protetto; la pena dell'arresto congiunta a quella dell'ammenda per le infrazioni che rechino un danno di particolare gravità. Il principio direttivo in commento consente quindi di derogare anche a tali limiti senza introdurne di nuovi. In proposito, si ricorda che la giurisprudenza costituzionale ha rilevato che il legislatore delegante, in ambito penale, deve adottare principi e criteri direttivi "configurati in modo assai preciso, sia definendo la specie e l'entità massima delle pene, sia dettando il criterio, in sé restrittivo, del ricorso alla sanzione penale solo per la tutela di determinati interessi rilevanti" (sentenza n. 175/2022. Precedenti: sent. n. 174/2021; sent. n. 127/2017; sent. n. 5/2014; sent. n. 49/1999; sent.

n. 53/1997). In questo ambito, infatti, il controllo sul rispetto di tali criteri e principi direttivi è "anche strumento di garanzia della riserva di legge e del rispetto del principio di stretta legalità, spettando al Parlamento l'individuazione dei fatti da sottoporre a pena e delle sanzioni loro applicabili".

Un secondo criterio di delega stabilisce (o meglio, sembra confermare) che gli **introiti derivanti dall'irrogazione delle sanzioni** siano versati all'entrata del bilancio dello Stato per essere riassegnati ad apposito capitolo dello stato di previsione della spesa del Ministero dell'economia per **incrementare la dotazione del bilancio dell'Agenzia** per la cybersicurezza nazionale;

Per quanto concerne la destinazione degli introiti delle sanzioni, si ricorda che ai sensi del decreto-legge n. 82/2021, già attualmente i proventi delle sanzioni irrogate dall'Agenzia ai sensi di quanto previsto dal decreto legislativo NIS e relative norme attuative, costituiscono entrate dell'Agenzia per la cybersicurezza nazionale (art. 11, co. 2, lett. f)).

- assicurare il **coordinamento** tra le disposizioni della direttiva (UE) NIS 2, quelle della direttiva (UE) 2022/2557 (c.d. direttiva CER) relativa alla resilienza dei soggetti critici, la cui delega è contenuta nell'articolo 4 della proposta di legge in esame, nonché del regolamento (UE) 2022/2554 (c.d. regolamento DORA) e della direttiva (UE) 2022/2556 in materia di servizi finanziari, la cui delega è contenuta nell'articolo 14 della medesima proposta (**lettera o**);

In proposito si ci limita a ricordare che la direttiva NIS 2 fa parte di un più ampio pacchetto di strumenti giuridici a livello dell'Unione, mirato a rafforzare i soggetti pubblici e privati rispetto alle minacce nell'ambito cibernetico. In particolare, per quanto qui rileva:

- la direttiva (UE) 2022/2557 (cosiddetta direttiva CER – *Critical Entities Resilience*) è relativa alla resilienza dei soggetti critici e interviene in abrogazione della precedente direttiva 2008/114/CE del Consiglio, concernente l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione;
- il Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* – DORA) definisce obblighi sulla sicurezza dei sistemi informatici e di rete che sostengono i processi commerciali delle entità finanziarie;
- la correlata direttiva (UE) 2022/2556 reca una serie di modifiche necessarie per rendere chiara e coerente l'applicazione, da parte delle entità finanziarie autorizzate e sottoposte a vigilanza conformemente a

tali direttive, dei vari requisiti di resilienza operativa digitale necessari per lo svolgimento delle loro attività e per la prestazione di servizi.

- apportare alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il **coordinamento** con le disposizioni emanate in attuazione dell'articolo in esame (**lettera p**).

CAPO I – DISPOSIZIONI GENERALI

Articoli 1 e 2
(Oggetto e definizioni)

L'**articolo 1** stabilisce come oggetto del provvedimento l'individuazione di un livello elevato di sicurezza informatica.
L'**articolo 2** reca le definizioni rilevanti per il provvedimento.

In particolare, il comma 2 dell'articolo 1 richiama i seguenti contenuti del provvedimento quali particolarmente rilevanti ai fini del perseguimento di un elevato livello di sicurezza informatica:

- la definizione di una strategia nazionale di cybersicurezza;
- l'integrazione del quadro di gestione delle crisi informatiche di cui all'articolo 10 del decreto-legge n. 82 del 2021 (tale articolo descrive le modalità di gestione delle crisi informatiche, soffermandosi in particolare sul ruolo del Nucleo per la Cybersicurezza costituito presso l'Agenzia per la cybersicurezza nazionale come struttura di supporto per il Presidente del Consiglio; il Nucleo è presieduto dal Direttore generale dell'Agenzia e composto dal Consigliere militare del Presidente del Consiglio e da rappresentanti del Dipartimento per le informazioni e la sicurezza e del Dipartimento della protezione civile; l'articolo 10 prevede ad esempio che il Nucleo mantenga costantemente informato il Presidente del Consiglio, assicuri il coordinamento per l'attuazione a livello interministeriale delle determinazioni del Presidente del Consiglio per il superamento delle crisi, raccolga i dati, elabori rapporti, fornisca informazioni e cooperi con i meccanismi europei di gestione delle crisi cibernetiche);
- la conferma dell'Agenzia per la cybersicurezza nazionale quale autorità nazionale competente nel settore; punto di contatto unico per i vari soggetti coinvolti e nei confronti dell'Unione europea e gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale (CSIRT Italia)
- la designazione dell'Agenzia per la cybersicurezza nazionale e del Ministero della difesa come autorità nazionali di gestione delle crisi informatiche su vasta scala; l'Agenzia e il Ministero agiranno ciascuno nel proprio ambito di competenza individuato dall'articolo 2, comma 1, lettera g) del provvedimento (vale a dire: ambito proprio del Ministero della

difesa è la difesa dello Stato; per il resto è competente l'Agenzia per la cybersicurezza nazionale); inoltre l'Agenzia svolgerà anche i compiti di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva oggetto di recepimento (che prescrive appunto che gli Stati membri se designano più autorità di gestione delle crisi informatiche devono però anche individuare un coordinatore);

- l'individuazione di autorità di settore che collaborano con l'Agenzia;
- l'individuazione di criteri per l'individuazione dei soggetti cui si applica il provvedimento e la definizione degli obblighi in materia di gestione del rischio informatico;
- la partecipazione a livello di Unione europea al gruppo di cooperazione NIS tra le autorità competenti in materia, alla Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) alla rete dei CSIRT nazionali.

L'articolo 2 reca le definizioni rilevanti per il provvedimento; le stesse saranno riprese nelle schede di lettura relative ai singoli articoli.

Articolo 3
(Ambito di applicazione)

L'**articolo 3** definisce l'ambito di applicazione del provvedimento, distinguendo i settori ritenuti, rispettivamente, altamente critici e critici, nonché i relativi sottosettori e tipi di soggetti di cui agli allegati I e II, le categorie delle pubbliche amministrazioni sottoposte alla nuova disciplina, di cui all'allegato III, e le ulteriori tipologie di soggetti a cui si applica il presente decreto, di cui all'allegato IV.
Al fine di superare l'attuale disomogeneità nel processo di identificazione dei soggetti da parte degli Stati membri, la disposizione introduce (ai commi 2, 3 e 4) il criterio di individuazione dei soggetti su base dimensionale (corrispondente alla c.d. "*sizecap rule*"), estendendo, rispetto al sistema delineato dalla direttiva NIS, l'applicazione della direttiva NIS 2 a tutte le medie e grandi imprese che operano nei settori di cui agli allegati I e II.
Alcuni soggetti sono inclusi nell'ambito applicativo del presente schema di decreto indipendentemente dalla loro dimensione, come nel caso di quelli di cui ai commi 5, 9 e 10, delle pubbliche amministrazioni di cui all'allegato III e dei soggetti elencati nell'allegato IV.

Ai sensi del **comma 1**, nell'ambito di applicazione del decreto rientrano i **soggetti pubblici e privati delle tipologie di cui agli allegati I, II, III e IV**, che sono sottoposti alla giurisdizione nazionale ai sensi del successivo articolo 5.

Si ricorda che la direttiva NIS 2 ha **ampliato,** rispetto a quanto previsto dalla previgente direttiva NIS, **il campo di applicazione della disciplina sulla sicurezza cibernetica**, da un lato includendovi anche la pubblica amministrazione centrale (lasciando discrezionalità agli Stati membri di inserire gli enti locali in base all'assetto istituzionale), le piccole e microimprese (solo se operano in settori chiave per la società) e, indipendentemente dalle dimensioni, fornitori di servizi di comunicazione elettroniche pubbliche e di reti di comunicazione elettronica accessibili al pubblico, e dall'altro lato, aumentando significativamente i settori di applicazione.

Inoltre, mentre ai sensi della direttiva NIS la responsabilità di determinare quali soggetti soddisfacessero i criteri per essere considerati operatori di servizi essenziali spettava agli Stati membri, la direttiva NIS 2 ha introdotto la **regola della soglia di dimensione**. Ciò significa che tutti i soggetti di medie e grandi dimensioni che operano nei settori o forniscono i servizi contemplati dalla direttiva dovrebbero rientrare nel suo ambito di applicazione.

Il nuovo regime **esclude** dalla sua applicazione i soggetti operanti in **settori** quali la sicurezza nazionale, la pubblica sicurezza o la difesa, il contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati. Sono altresì esclusi Parlamenti e banche centrali.

Gli allegati I e II descrivono i settori ritenuti, rispettivamente, altamente critici e critici, nonché i relativi sottosettori e le tipologie di soggetti.

Quelli individuati all'**allegato I** come **settori ad alta criticità** sono i seguenti:

1. Energia (comprensivo dei sottosettori dell'energia elettrica (a), del teleriscaldamento e teleraffrescamento (b), del petrolio (c), del gas (d) e dell'idrogeno (e));
2. Trasporti (comprensivo dei sottosettori del trasporto aereo (a), del trasporto ferroviario (b), del trasporto per vie d'acqua (c) e del trasporto su strada (d));
3. Settore bancario;
4. Infrastrutture dei mercati finanziari;
5. Settore sanitario;
6. Acqua potabile;
7. Acque reflue;
8. Infrastrutture digitali;
9. Gestione dei servizi TIC (*business-to-business*);
10. Spazio.

L'**allegato II** individua i seguenti quali **altri settori critici**:

1. Servizi postali e di corriere;
2. Gestione dei rifiuti;
3. Fabbricazione, produzione e distribuzione di sostanze chimiche;
4. Produzione, trasformazione e distribuzione di alimenti;
5. Fabbricazione (comprensivo dei sottosettori della fabbricazione di dispositivi medici e di dispositivi medicodiagnostici in vitro (a), della fabbricazione di computer e prodotti di elettronica e ottica (b), della fabbricazione di apparecchiature elettriche (c), della fabbricazione di macchinari e apparecchiature n.c.a. (d), della fabbricazione di autoveicoli, rimorchi e semirimorchi (e) e della fabbricazione di altri mezzi di trasporto (f)):
6. Fornitori di servizi digitali;
7. Ricerca.

Gli allegati III e IV descrivono, rispettivamente, le categorie di pubbliche amministrazioni e le ulteriori tipologie di soggetti a cui si applica il decreto in esame.

Secondo l'**allegato III**, rientrano nell'ambito di applicazione del decreto:

a) le seguenti amministrazioni centrali:
   1. gli Organi costituzionali e di rilievo costituzionale;
   2. la Presidenza del Consiglio dei ministri e i Ministeri;
   3. le Agenzie fiscali;
   4. le Autorità amministrative indipendenti;

Dall'applicazione del provvedimento sono però esclusi, ai sensi dell'articolo 4, comma 2, Camera dei deputati e Senato della Repubblica; anche gli altri organi costituzionali e di rilievo costituzionale sono inoltre esclusi, sempre ai sensi dell'articolo 4, comma 2, dall'applicazione delle disposizioni del Capo V in materia di monitoraggio, vigilanza ed esecuzione.

b) le amministrazioni regionali, vale a dire le Regioni e le Province autonome;

c) le amministrazioni locali, vale a dire:
   1. le Città metropolitane;
   2. i Comuni con popolazione superiore a 100.000 abitanti;
   3. i Comuni capoluoghi di regione;
   4. le Aziende sanitarie locali;

d) altri soggetti pubblici, tra cui:
   1. gli Enti di regolazione dell'attività economica;
   2. gli Enti produttori di servizi economici;
   3. gli Enti a struttura associativa;
   4. gli Enti produttori di servizi assistenziali, ricreativi e culturali;
   5. gli Enti e le Istituzioni di ricerca;
   6. gli Istituti zooprofilattici sperimentali.

Gli ulteriori soggetti individuati all'**allegato IV** sono:
1. i soggetti che forniscono servizi di trasporto pubblico locale;
2. gli istituti di istruzione che svolgono attività di ricerca;
3. i soggetti che svolgono attività di interesse culturale;
4. le società *in house*, le società partecipate e le società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175.

Per quanto riguarda i **soggetti delle tipologie di cui all'allegato I e II**, il **comma 2** stabilisce che il decreto si applica **solo a quelli che superano i massimali per le piccole imprese** ai sensi dell'articolo 2, paragrafo 2, dell'allegato alla raccomandazione della Commissione relativa alla definizione delle microimprese, piccole e medie imprese (2003/361/CE).

Secondo l'articolo 2, paragrafo 2, dell'allegato alla raccomandazione citata, nella categoria delle PMI si definisce **piccola impresa** un'impresa che occupa **meno di**

50 persone e realizza un fatturato annuo o un totale di bilancio annuo **non superiori a 10 milioni di euro**.

Il **comma 3** esclude invece l'applicazione, ai fini del provvedimento in esame, dell'articolo 3, paragrafo 4, dell'allegato alla raccomandazione 2003/361/CE.

Tale disposizione stabilisce che un'impresa non può essere considerata PMI se almeno il 25% del suo capitale o dei suoi diritti di voto è controllato direttamente o indirettamente da uno o più organismi collettivi pubblici o enti pubblici, a titolo individuale o congiuntamente.

Il **comma 4** prevede che, al fine di determinare se un soggetto sia o meno da considerarsi una media o grande impresa ai sensi dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE, si applica l'articolo 6, paragrafo 2, del medesimo allegato, secondo il quale

«Per le imprese associate o collegate, i dati, inclusi quelli relativi agli effettivi, sono determinati sulla base dei conti e di altri dati dell'impresa oppure, se disponibili, sulla base dei conti consolidati dell'impresa o di conti consolidati in cui l'impresa è ripresa tramite consolidamento.

Ai dati di cui al primo comma si aggregano i dati delle eventuali imprese associate dell'impresa in questione, situate immediatamente a monte o a valle di quest'ultima. L'aggregazione è effettuata in proporzione alla percentuale di partecipazione al capitale o alla percentuale di diritti di voto detenuti (si sceglie la percentuale più elevata fra le due). Per le partecipazioni incrociate si applica la percentuale più elevata.

Ai dati di cui al primo e al secondo comma si aggiunge il 100% dei dati relativi alle eventuali imprese direttamente o indirettamente collegate all'impresa in questione che non siano già stati ripresi nei conti tramite consolidamento».

All'applicazione di tale disposizione si procede salvo che l'effetto non risulti sproporzionato, tenuto anche conto dell'indipendenza del soggetto dalle sue imprese collegate in termini di sistemi informativi e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce.

Il **comma 5** reca l'elenco dei soggetti a cui il decreto in esame si applica, indipendentemente dalle loro dimensioni. Si tratta, in particolare, dei:

a) soggetti che sono identificati come soggetti critici ai sensi del decreto legislativo, che recepisce la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022 (in termini sintetici, si tratta dei soggetti che operano nei servizi essenziali, esclusi quelli della sicurezza nazionale, della pubblica sicurezza, della difesa, della prevenzione e contrasto dei reati; lo schema di decreto legislativo di

recepimento di tale direttiva, atto n. 165, è anch'esso all'esame delle Camere);
b) fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico;
c) prestatori di servizi fiduciari;
d) gestori di registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;
e) fornitori di servizi di registrazione dei nomi di dominio.

Il **comma 6** stabilisce che anche alle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III, il presente decreto si applica indipendentemente dalle loro dimensioni.

In virtù di quanto previsto al **comma 7**, con uno o più decreti del Presidente del Consiglio dei ministri adottati secondo le modalità di cui all'articolo 40, comma 2, possono essere individuate ulteriori categorie di pubbliche amministrazioni a cui si applica il presente decreto al fine di adeguare l'elenco di categorie di cui all'allegato III.

L'individuazione deve avvenire sulla base di un criterio di gradualità, dell'evoluzione del grado di esposizione al rischio della pubblica amministrazione, della probabilità che si verifichino incidenti e della loro gravità, compreso il loro impatto sociale ed economico, tenuto conto anche dei criteri di cui al comma 9 dell'articolo in esame.

Secondo il **comma 8**, il presente decreto si applica anche ai soggetti delle tipologie di cui all'allegato IV, individuati secondo le procedure di cui al comma 13, indipendentemente dalle loro dimensioni.

Il **comma 9** definisce le condizioni a cui il presente decreto si applica, indipendentemente dalle loro dimensioni, anche ai soggetti dei settori o delle tipologie di cui agli allegati I, II, III e IV, individuati secondo le procedure di cui al comma 13. Ciò avviene, in particolare, qualora:
a) il soggetto sia identificato prima della data di entrata in vigore del presente decreto come operatore di servizi essenziali ai sensi del decreto legislativo 18 maggio 2018, n. 65;
b) il soggetto sia l'unico fornitore nazionale di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
c) una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;

d) una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;
e) il soggetto sia critico in ragione della sua particolare importanza a livello nazionale o regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nel territorio dello Stato;
f) il soggetto sia considerato critico ai sensi del presente decreto quale elemento sistemico della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti.

Infine, il **comma 10** prevede che il presente decreto si applichi, indipendentemente dalle sue dimensioni, anche all'impresa collegata ad un soggetto essenziale o importante, laddove essa soddisfi almeno uno dei seguenti criteri:
a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;
b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;
c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale;
d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.

Resta ferma la disciplina in materia di protezione dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e al decreto legislativo 30 giugno 2003, n. 196, **nonché in materia di lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile** di cui al decreto legislativo 4 marzo 2014, n. 39 (**comma 11**).

L'Autorità nazionale competente NIS applica la clausola di salvaguardia di cui al comma 4, secondo i criteri per la determinazione individuati con le modalità di cui all'articolo 40, comma 1 (**comma 12**).

Secondo il **comma 13**, i soggetti di cui ai commi 8 e 9 sono individuati dall'Autorità nazionale competente NIS, su proposta delle Autorità di settore, secondo le modalità di cui all'articolo 40, comma 4.
L'Autorità nazionale competente NIS notifica a tali soggetti la loro individuazione ai fini della registrazione di cui all'articolo 7, comma 1.

Le disposizioni di cui all'**articolo 17** e ai **Capi IV e V** del presente decreto **non si applicano** ai **soggetti** identificati come **essenziali o importanti** dei

settori 3 e 4 di cui all'**allegato I**, ai quali si applica la disciplina di cui al regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario (**comma 14**).

Il **comma 15** stabilisce che, ai sensi dell'articolo 2, comma 10, della direttiva, il decreto non si applica ai soggetti esentati dall'ambito di applicazione del regolamento (UE) 2022/2554, relativo alla resilienza operativa digitale per il settore finanziario.

Articolo 4
(Protezione degli interessi nazionali e commerciali)

L'**articolo 4** chiarisce essenzialmente a quali ambiti lo schema di decreto legislativo **non si applica**.

Composto di **8 commi** e ricco di rinvii ad altre fonti di rango primario, l'art. 4 dello schema in commento – facendo seguito all'art. 3 che ne delinea l'ambito d'applicazione - si occupa di **esplicitare l'esclusione una cospicua serie di ambiti** dall'applicazione delle norme di recepimento della direttiva NIS2.

Da questo punto di vista, il **comma 1** dello schema fa eco ai ***Considerando* 9 e 11** della **direttiva**, secondo cui – tra l'altro - "gli Stati membri dovrebbero poter **esentare soggetti specifici** che svolgono attività nei settori della **sicurezza nazionale, della pubblica sicurezza, della difesa o dell'applicazione della legge**, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati da determinati obblighi previsti dalla presente direttiva per quanto riguarda tali attività. Qualora un soggetto fornisca servizi esclusivamente a un ente della pubblica amministrazione escluso dall'ambito di applicazione della presente direttiva, gli Stati membri dovrebbero poter esentare tale soggetto da determinati obblighi stabiliti dalla presente direttiva per quanto riguarda tali servizi. Inoltre, nessuno Stato membro dovrebbe essere tenuto a fornire **informazioni la cui divulgazione sia contraria agli interessi essenziali della propria pubblica sicurezza**. Dovrebbero essere prese in considerazione in tale contesto le norme dell'Unione o nazionali per la protezione delle informazioni classificate, gli accordi di non divulgazione o gli accordi di non divulgazione informali, quale il protocollo TLP".

Sono, quindi, esclusi dall'ambito di applicazione della nuova normativa, nonostante possano essere considerate *lato sensu* pubbliche amministrazioni, ai sensi del predetto art. 3:

- il **Parlamento**;
- l'**autorità giudiziaria**;
- la **Banca d'Italia** e l'**UIF.**

Viene precisato inoltre che gli **organi costituzionali** e quelli di **rilievo costituzionale** sono esclusi dall'applicazione del **capo V**, che inerisce alle misure di monitoraggio, vigilanza ed esecuzione.

Ai sensi del **comma 3**, sono altresì esclusi dalla nuova normativa gli enti, gli organi e le articolazioni della pubblica amministrazione che operano nei settori:

i) della **pubblica sicurezza**;

ii) della **difesa nazionale**;

iii) dell'attività di **contrasto**, compresa l'indagine, l'accertamento e il perseguimento, **di reati**;

né ancora

iv) agli organismi d'**informazione di sicurezza dello Stato**;

v) all'**ACN**.

Al **comma 4**, si attribuisce a una **fonte secondaria** (uno o più **d.P.C.M**., d'intesa o su proposta dei Ministri della giustizia, interno e difesa e d'intesa con l'ACN) il compito di individuare **quali soggetti siano** da ricomprendere nel **perimetro** di quanti forniscono ai predetti soggetti esclusi **beni e servizi in via esclusiva**, di modo che costoro, a loro volta, siano esclusi dall'applicazione dei capi IV e V del decreto legislativo in via di approvazione.

A questa regola appaiono essere apportate due **precisazioni**:

- il d.P.C.M. può inerire anche alla fornitura in esclusiva a pubbliche amministrazioni incaricate della **protezione civile**.

*Sotto questo aspetto, si valuti di **coordinare il disposto** dei commi **3** e **4**.*

- l'individuazione dei fornitori in via esclusiva dei **servizi d'informazione** – **esclusa** l'**Aisi** – è fatta con **d.P.R**. e non con d.P.C.M.

Al **comma 6**, è detto – però – che la fornitura esclusiva non dà luogo all'esclusione dall'ambito di applicazione del decreto legislativo se si tratta di attività **solo marginalmente** connesse a quelle d'istituto dell'organo di cui si tratta; né possono essere esclusi i **soggetti fiduciari** (v. la scheda all'art. **3, comma 1, lett. *ss***).

Al **comma 7** è stabilito un principio generale d'**ispirazione** e d'**interpretazione** di tutto il decreto legislativo, in coerenza peraltro con l'art. **346** TFUE: ovunque esso preveda **obblighi di ostensione e d'informazione**, tali obblighi non possono **mai** comportare la **divulgazione d'informazioni sensibili per gli interessi essenziali** dello Stato.

Il comma 8 – analogamente – precisa che, laddove la normativa UE o interna preveda lo scambio d'informazioni con la Commissione europea (v., per esempio, l'art. **22** del provvedimento in commento), questo deve avvenire sempre secondo il principio di proporzione e in modo da non pregiudicare gli interessi e la riservatezza dei soggetti **essenziali** e dei soggetti **importanti** (per tali definizioni v. gli artt. 6, 7, 24 e 30).

Articolo 5
(Giurisdizione e territorialità)

L'**articolo 5** individua, sostanzialmente riproducendo il contenuto dell'articolo 26 della direttiva, i criteri per definire a quale **giurisdizione** siano assoggettati i soggetti, individuati dall'articolo 3, che rientrano nell'ambito di applicazione del presente provvedimento.

Il **comma 1** prevede in via generale che tali soggetti sono sottoposti alla **giurisdizione nazionale dello Stato membro nel quale sono stabiliti** con le eccezioni che seguono:

- sono considerati sottoposti alla **giurisdizione dello Stato membro nel quale forniscono i loro servizi:**
  - i fornitori di reti pubbliche di comunicazione elettronica;
  - i fornitori di servizi di comunicazione elettronica accessibili al pubblico;
- sono considerati sottoposti alla **giurisdizione dello Stato membro in cui hanno lo stabilimento principale:**
  - fornitori di servizi di sistema dei nomi di dominio DNS, i registri dei nomi di dominio di primo livello;
  - i soggetti che forniscono servizi di registrazione dei nomi di dominio;
  - i fornitori di servizi di *cloud computing*;
  - i fornitori di servizi di data center;
  - i fornitori di reti di distribuzione dei contenuti;
  - i fornitori di servizi gestiti;
  - i fornitori di servizi di sicurezza gestiti;
  - i fornitori di mercati *online*, di motori di ricerca online o di piattaforme di servizi di *social network*;
- sono considerati sottoposti alla **giurisdizione dello Stato membro che li ha istituiti:**
  - gli enti della pubblica amministrazione.

Il **comma 2** specifica che si considera **stabilimento principale nell'Unione** quello dello Stato membro nel quale sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio per la sicurezza informatica. Qualora non sia possibile determinare lo Stato membro in cui sono adottate tali decisioni o se queste non sono adottate nell'Unione, lo stabilimento principale è considerato quello collocato nello Stato membro in cui sono effettuate le operazioni di sicurezza informatica.

Qualora anche in base a quest'ultimo criterio non sia possibile individuare lo Stato membro, allora si considera lo Stato membro in cui il soggetto interessato ha lo stabilimento con il maggior numero di dipendenti nell'Unione europea.

Con riferimento ai fornitori di servizi digitali che non sono stabiliti nell'Unione europea, ma offrono servizi all'interno dell'Unione europea, si prevede l'obbligo di designare un **rappresentante nell'Unione europea**, che è stabilito in uno di quegli Stati membri in cui sono offerti i servizi (**comma 3**).

Nell'**assenza di un rappresentante** nell'Unione designato, l'Autorità nazionale competente NIS può avviare un'**azione legale** nei confronti dei soggetti inadempienti (**comma 4**).

Ai sensi del **comma 5** la designazione del rappresentante fa salve le **azioni legali** che potrebbero essere già avviate per violazioni degli obblighi di cui al presente decreto, l'imposizione degli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente (di cui al capo IV) e l'esercizio dei poteri in materia di monitoraggio, vigilanza ed esecuzione (di cui al capo V).

Articolo 6
(Soggetti essenziali e soggetti importanti)

L'**articolo 6** individua i soggetti essenziali e importanti, in base ai requisiti dimensionali e alla tipologia di prodotti o servizi forniti.

Si ricorda in proposito che le categorie di 'soggetti essenziali' e di 'soggetti importanti', che la norma in commento definisce, sostituiscono nella direttiva NIS 2 la precedente categorizzazione di "operatori di servizi essenziali" e "fornitori di servizi essenziali". Così facendo si amplia il campo di applicazione della direttiva NIS rispetto al passato.

La **Direttiva NIS 2** supera l'impostazione della precedente direttiva legata ai concetti di "operatore di servizi essenziali" e di "fornitore di servizi digitali", liberamente identificati dagli Stati membri attraverso criteri disomogenei, stabilendo, invece, alcuni criteri uniformi per permettere una organica identificazione degli operatori pubblici e privati da includere in due nuove categorie di attori: quella dei "soggetti essenziali" (articolo 3, paragrafo 1) e quella dei "soggetti importanti" (articolo 3, paragrafo 2). Entro il 17 aprile 2025, gli Stati membri devono definire un **elenco** dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio, da riesaminare e aggiornare ogni due anni. Ai fini della compilazione dell'elenco, gli Stati membri impongono a tali soggetti di presentare alle autorità competenti le seguenti informazioni: nome; indirizzo e recapiti aggiornati; se del caso, i settori e sottosettori pertinenti di cui all'allegato I o II; se del caso, un elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione della direttiva.

Nella **categoria dei soggetti essenziali** ricadono, ai sensi del **comma 1**:

a) i **soggetti** di cui all'allegato I (ossia i soggetti presenti nei **settori ad alta criticità:** energia, trasporti, settore bancario, infrastrutture dei mercati finanziari, settore sanitario, acqua potabile, acque reflue, infrastrutture digitali, gestione dei servizi TIC e spazio) che **superano i massimali per le medie imprese** di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE. Tale categoria è prevista esplicitamente dalla direttiva (art. 3, co. 1, lett. a);

La **Raccomandazione della Commissione del 6 maggio 2003, n. 2003/361/CE** è relativa alla definizione delle microimprese, piccole e medie imprese C(2003) e dispone, in primo luogo, che è impresa ogni entità, a prescindere dalla forma giuridica rivestita, che eserciti un'attività economica.

Definisce poi come PMI, le imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di euro oppure il cui totale di bilancio annuo non supera i 43 milioni di euro (art. 2, par. 1, allegato).

In questo ambito:

- definisce piccola impresa un'impresa che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni;
- definisce micro-impresa un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni.

b) i soggetti identificati come **soggetti critici** ai sensi del decreto legislativo che recepisce la direttiva (UE) 2022/2557, **indipendentemente dalle loro dimensioni**, che è attualmente all'esame delle Camere (A.G. 165). Tale categoria è prevista esplicitamente dalla direttiva (art. 3, co. 1, lett. f);

Ai sensi dello schema di decreto richiamato, il **soggetto critico** è un soggetto pubblico o privato, appositamente individuato dalle autorità settoriali competenti, fornitore di un servizio essenziale, nei settori di attività cui si riferisce la direttiva. Ulteriori elementi definitori – quale la collocazione del soggetto e della sua infrastruttura critica, in tutto o in parte nel territorio nazionale – si rinvengono nell'articolo 8 dello schema, relativo al procedimento di loro individuazione.

c) i **fornitori di reti pubbliche** e i fornitori di **servizi di comunicazione elettronica** accessibili al pubblico di cui all'articolo 3, comma 5, lettera b), che si considerano medie imprese ai sensi dell'articolo 2 dell'allegato alla citata raccomandazione 2003/361/CE. Anche tale categoria è prevista esplicitamente dalla direttiva (art. 3, co. 1, lett. *c)*;

d) i **prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio** di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio di cui all'articolo 3, comma 5, lettere c) e d), indipendentemente dalle loro dimensioni: categoria prevista dalla direttiva all'art. 3, co. 1, lett. b);

e) le **pubbliche amministrazioni centrali** di cui all'allegato III, lettera a), ossia gli Organi costituzionali e di rilievo costituzionale; la Presidenza del Consiglio dei ministri e i Ministeri; le Agenzie fiscali e le Autorità amministrative indipendenti, tutte indipendentemente dalle loro dimensioni.

Ai sensi del **comma 2** rientrano ancora nella categoria dei **soggetti essenziali**, indipendentemente dalle loro dimensioni, come **individuati dall'Autorità nazionale competente NIS**[3]:

- le pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III (art. 3, co. 6);
- i soggetti delle tipologie di cui all'allegato IV, ossia: soggetti che forniscono servizi di trasporto pubblico locale; istituti di istruzione che svolgono attività di ricerca; soggetti che svolgono attività di interesse culturale, società in house, società partecipate e società a controllo pubblico, come definite nel D.Lgs. n. 175/2016 (art. 3, co. 8);
- i soggetti delle tipologie di cui agli allegati I (settori ad alta criticità), II (settori critici) e IV (ulteriori tipologie di soggetti), indipendentemente dalle loro dimensioni, laddove soddisfino determinati requisiti (art. 3, co. 9);
- le imprese collegate ad un soggetto essenziale o importante, se soddisfa determinati requisiti (art. 3, co. 10).

Il **comma 3** individua, in via residuale, la categoria dei **soggetti importanti**, facendovi rientrare tutti i soggetti pubblici e privati che rientrano nell'ambito di applicazione del decreto (di cui all'articolo 3) che non sono considerati essenziali ai sensi dei commi 1 e 2 dell'articolo in esame.

[33] L'individuazione va fatta con le modalità di cui all'articolo 40, comma 5, dello schema di decreto in esame, ovverosia con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS.

Articolo 7
(Identificazione ed elencazione dei soggetti essenziali e importanti)

L'**articolo 7** prevede il **procedimento** con cui sono identificati i soggetti **importanti** ed **essenziali**.

L'art. **7** dello schema in commento – facendo seguito all'art. 6, che **definisce** in via in generale i soggetti **importanti** ed **essenziali** - si occupa di **disciplinare il procedimento** con cui tali soggetti sono inseriti nei relativi noveri.

Da questo punto di vista, è previsto uno **scadenziario annuale**, in cui:

- i **soggetti destinatari** delle norme del decreto legislativo (v. *supra* la scheda all'art. **3**) sono chiamati a **registrarsi** su una **piattaforma predisposta** dall'**ACN**, indicando una serie d'**informazioni identificative** del soggetto che si registra (entro il **28 febbraio**);
- l'**ACN** deve compilare l'elenco dei soggetti importanti ed essenziali e comunicare l'inserimento ai soggetti interessati (entro il **31 marzo**);
- i soggetti inseriti devono comunicare o aggiornare le informazioni inerenti agli aspetti delle **comunicazioni elettroniche** (indirizzi IP, nomi di dominio, indirizzi di posta elettronica, recapiti, eccetera) (tra il **15 aprile** e il **31 maggio**);
- per gli adempimenti da svolgere tra il **1° maggio e il 30 giugno** di ciascun anno si veda la scheda all'articolo 30.

A prescindere dall'inserimento negli elenchi, il **comma 5** impone ai:

- **fornitori di servizi di sistema** dei nomi di dominio;
- **gestori di registri** di nomi di dominio di primo livello;
- **fornitori di servizi di registrazione** dei nomi di dominio;
- **fornitori** di servizi di ***cloud computing*;**
- **fornitori** di servizi di ***data center*;**
- **fornitori** di **reti** di distribuzione dei contenuti;
- **fornitori** di servizi **gestiti**;
- **fornitori** di servizi di **sicurezza** gestiti;
- **fornitori** di **mercati *on line***;
- **fornitori** di **motori di ricerca *on line***;
- **fornitori** di **piattaforme di *social network***

di comunicare all'ACN l'indirizzo della sede principale e delle altre sedi nell'UE o – se si tratti di soggetti *extra* UE – l'indirizzo e i recapiti della sede del rappresentante in UE.

Le modificazioni delle informazioni già trasmesse sulla piattaforma devono essere trasmesse entro **14 giorni** dall'avvenuta modifica.

Per le modalità di adempimento degli obblighi illustrati, si veda la scheda relativa all’articolo 40.

Articolo 8
(Protezione dei dati personali)

L'**articolo 8** riguarda il **trattamento dei dati personali** rinviando, quanto alla disciplina applicabile, al **codice della *privacy*** e alla **legislazione dell'Unione europea** in materia di trattamento dei dati personali e **tutela della vita privata e comunicazioni elettroniche**.

Il **comma 1** dispone che l'Agenzia per la cybersicurezza nazionale, le Autorità di settore NIS (*sulle quali si veda l'art. 11*) e i soggetti pubblici e privati che rientrano nell'ambito di applicazione della disciplina recata dallo schema di decreto in esame (indicati all'articolo 3) **trattano i dati personali in misura necessaria** ai fini del provvedimento in commento e **conformemente al codice della *privacy*** di cui al d. lgs. 196/2003 e al **regolamento GDPR** (regolamento (UE) 2016/679).

Il regolamento generale sulla protezione dei dati (GDPR) si applica a tutte le organizzazioni che trattano dati personali di cittadini dell'Unione europea, indipendentemente dal fatto che l'organizzazione sia situata all'interno o all'esterno dell'Unione. I **principi** relativi al trattamento dei dati personali sanciti dal Regolamento sono liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione e integrità e riservatezza. Tali principi determinano, pertanto, che i dati devono essere trattati in modo lecito, raccolti per finalità specifiche, limitati a quanto necessario, esatti e aggiornati, conservati solo per il tempo necessario e trattati in modo sicuro.

Il regolamento GDPR riconosce altresì una serie di **diritti** ai titolari dei dati personali. Questi ultimi hanno il diritto di essere informati del trattamento dei loro dati e di accedere a agli stessi (diritto di accesso), di richiedere la correzione di dati inesatti (diritto di rettifica), di chiedere la cancellazione dei propri dati personali (diritto alla cancellazione o "diritto all'oblio"), di chiedere la limitazione del trattamento dei loro dati (diritto alla limitazione del trattamento), di ricevere i propri dati in un formato strutturato e leggibile da dispositivo automatico (diritto alla portabilità dei dati) e di opporsi al trattamento dei propri dati in determinate circostanze (diritto di opposizione).

Per quanto riguarda gli **obblighi per i titolari del trattamento**, il regolamento GDPR richiede che questi siano in grado di dimostrare la conformità al regolamento (responsabilità). Le misure di protezione dei dati, inoltre, devono essere integrate sin dall'inizio della progettazione dei processi (*privacy by design* e by *default*).

Il GDPR disciplina anche i **trasferimenti internazionali di dati**, stabilendo che i dati personali possono essere trasferiti al di fuori dell'UE solo verso paesi che offrono un livello di protezione adeguato o mediante l'adozione di strumenti giuridici appropriati.

Il codice della privacy di cui al d.lgs 196/2003, a seguito delle modifiche apportate dal d.lgs. 101/2018, recepisce i contenuti del regolamento GDPR, garantendo così la coerenza tra la normativa europea e quella nazionale in materia di protezione dei dati personali.

Il **comma 2** riguarda il **trattamento dei dati personali** da parte dei **fornitori di reti pubbliche di comunicazione elettronica** e di **fornitori di servizi di comunicazione elettronica accessibili al pubblico**, prevedendo che il trattamento venga effettuato conformemente alla legislazione dell'Unione europea in materia di trattamento dei dati personali e di **tutela della vita privata**, ai sensi della direttiva 58/2002/CE relativa alla vita privata e alla comunicazione elettronica.

Secondo quanto disposto dall'art. 2, comma 1, lettera *tt)* del **Codice delle comunicazioni elettroniche** (decreto legislativo n. 259 del 2003) per **rete pubblica di comunicazione elettronica** si intende una rete di comunicazione elettronica, utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica **accessibili al pubblico**, che supporta il trasferimento di informazioni tra i punti terminali di rete.

Ne deriva che sono **fornitori di reti pubbliche di comunicazione elettronica** coloro che mettono a disposizione del pubblico servizi di comunicazione elettronica **su reti pubbliche.**

Ai sensi dell'art. 2, comma 1, lettera fff), del medesimo Codice per **servizi di comunicazione elettronica** si intendono i servizi, forniti di norma a pagamento su reti di comunicazioni elettroniche, che comprendono, con l'eccezione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti, i seguenti tipi di servizi:

1) servizio di accesso a *internet*;
2) servizio di comunicazione interpersonale;
3) servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali, come i servizi di trasmissione utilizzati per la fornitura di servizi da macchina a macchina e per la diffusione circolare radiotelevisiva.

CAPO II – QUADRO NAZIONALE DI SICUREZZA INFORMATICA

Articolo 9
(Strategia nazionale di cybersicurezza)

L'**articolo 9** stabilisce che spetta alla Strategia nazionale di cybersicurezza individuare obiettivi, risorse, elementi e misure strategiche per raggiungere e mantenere un alto grado di tutela della sicurezza delle reti e dei sistemi di interesse nazionale; la norma dispone, altresì, le modalità di valutazione e aggiornamento della Strategia nazionale della cybersicurezza.

L'**articolo 9** risponde all'obbligo contenuto all'**articolo 7** della direttiva (UE) 2022/2555 di imporre a tutti gli Stati Membri l'adozione di una Strategia nazionale di cybersicurezza. In particolare, l'articolo in commento aggiorna quanto già previsto in materia dall'abrogando decreto legislativo del 18 maggio 2018, n. 65 (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) – c.d. NIS – così come modificato ed integrato dal decreto legge del 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 legge 4 agosto 2021, n. 109.

Il decreto legge n. 82 del 2021 è intervenuto sostanzialmente nel ridefinire l'architettura nazionale in materia di cybersicurezza ed ha istituito l'Agenzia per la cybersicurezza nazionale per la tutela degli interessi nazionali nel campo di riferimento attraverso l'adempimento di alcuni funzioni tra cui, in primo luogo, proprio la predisposizione della Strategia nazionale di cibersicurezza.

Per quel che concerne quest'ultima, il suo sistema di *governance* è stato modificato dal decreto legge n. 82/2021 che ne ha precisato i contenuti, in attuazione dell'abrogando decreto legislativo n. 65 del 2018. Il medesimo decreto legge, all'**articolo 15, primo comma, lettera a),** ha modificato poi il decreto legislativo NIS sostituendo le parole: «strategia nazionale di sicurezza cibernetica» con le seguenti: «strategia nazionale di cybersicurezza».

Riguardo al decreto legislativo NIS, invece, si ricorda che il relativo **articolo 6** statuisce che sia Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la cybersicurezza (CIC), ad adottare la Strategia.

Si ricorda che il CIC è istituito dall'**articolo 4** del decreto legge del 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) presso la Presidenza del Consiglio dei ministri con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. Si segnala, inoltre, che l'intervento del CIC nella determinazione della Strategia è una diretta conseguenza degli emendamenti apportati dal decreto legge n. 82 del 2018 al decreto legislativo NIS. In particolare si tratta del combinato disposto dell'articolo 2, che conferma la competenza esclusiva del Presidente del Consiglio nell'adottare la strategia ma sostituisce il parere del CISR[4] con quello del CIC, e dell'articolo 4, con il quale viene istituito quest'ultimo.

La Strategia è poi attuata, ai sensi dell'**articolo 7, comma 1, lettera b),** del medesimo decreto legislativo dall'Agenzia per la cybersicurezza nazionale.

Lo schema di decreto legislativo in esame, invece, definisce all'**articolo 2** la Strategia come "il quadro coerente che prevede obiettivi strategici e priorità in materia di cybersicurezza e la *governance* per il loro conseguimento"

Di questi ultimi si occupa l'**articolo 9** in commento, il cui **comma 1** stabilisce che la Strategia nazionale di cybersicurezza individua obiettivi, risorse e misure per raggiungere e mantenere un alto grado di tutela della sicurezza delle reti e dei sistemi di interesse nazionale.

Gli elementi della strategia sono materia, invece, del **comma 2**. In particolare, si tratta di:

a) **obiettivi e priorità** che interessano soprattutto i settori di cui agli allegati I, II, III e IV;

Tali allegati contengono gli elenchi dei soggetti a rischio individuati su base dimensionale nel rispetto della c.d. "*sizecap rule*" introdotta dalla direttiva NIS 2 e recepita dallo schema di decreto legislativo in commento e che ha, di fatto, esteso l'applicazione della norma a tutte le medie e grandi imprese che operano nei settori altamente critici, di cui all'allegato I, e quelli critici, di cui all'allegato II[5]. Dalla

[4] Il testo originario dell'articolo 6 del decreto legislativo n. 65 del 2018 prevedeva, infatti, che il Presidente del Consiglio dovesse sentire il Comitato interministeriale per la sicurezza della Repubblica (CISR) ovvero l'organismo di consulenza, proposta e deliberazione sugli indirizzi e le finalità generali della politica dell'informazione per la sicurezza. In particolare il Comitato: delibera sulla ripartizione delle risorse finanziarie e sui bilanci preventivi e consuntivi di DIS, AISE e AISI; indica il fabbisogno informativo necessario ai ministri per svolgere l'attività di governo.

[5] L'allegato I comprende i soggetti che operano, in particolare, nella pubblica amministrazione e nei settori e nei sotto settori: dell'energia, dei trasporti, bancari, delle infrastrutture dei mercati

direttiva vengono altresì comprese tutte quelle imprese che, a prescindere dalle loro dimensioni, ricoprono un ruolo chiave per la società o per l'economia nazionale o sono espressamente menzionati nella direttiva NIS 2 e che nello schema di decreto legislativo vengono menzionate dall'allegato IV come "ulteriori tipologie di soggetti".

Si segnala che, precedentemente e nel rispetto della direttiva NIS 1, le imprese interessate erano solo quelle identificate come produttrici di servizi essenziali creando però disomogeneità tra i diversi Stati Membri.

I settori di cui all'allegato III, invece, comprendono le amministrazioni centrali, regionali, locali e di altro tipo.

b) un **quadro di *governance* per la realizzazione degli obiettivi** e delle priorità di cui sopra alla lettera a) e che comprenda anche le **misure strategiche** elencate dal successivo comma 3 (*infra*);
c) un **quadro di *governance* che contenga una descrizione dei ruoli e delle responsabilità** di tutte le parti coinvolte, tra cui organismi pubblici e soggetti portatori di interesse, nell'attuazione della strategia al fine di migliorare il coordinamento e la cooperazione;
d) un **meccanismo per individuare le risorse** e una **valutazione dei rischi** a livello nazionale;
e) **misure volte a garantire la preparazione, la risposta e il recupero** da incidenti che comprendano anche la collaborazione tra o settori pubblico e privato;
f) un **elenco dei soggetti coinvolti** nell'attuazione della strategia;
g) un **quadro strategico per il coordinamento rafforzato** tra le autorità competenti per la condivisione di informazioni sui rischi e per la vigilanza;
h) un **piano che contenga misure atte ad incrementare nei cittadini il livello di consapevolezza** in materia di cybersicurezza;

Le **misure strategiche** introdotte nell'ambito della Strategia nazionale per la cybersicurezza sono elencate dal **comma 3** e riguardano, in particolare:

a) la **sicurezza informatica nella catena di approvvigionamento dei prodotti e dei servizi TIC** (tecnologie dell'informazione e della comunicazione) utilizzati dai soggetti per la fornitura dei loro servizi;
b) l'**inclusione e la definizione dei requisiti** concernenti la sicurezza informatica per i prodotti e servizi TIC negli appalti pubblici;

finanziari, della distribuzione delle acque potabile o della raccolta e smaltimento di quelle reflue, delle infrastrutture digitali, della gestione dei servizi TIC, della gestione delle strutture e servizi per lo spazio.
L'allegato II, invece, comprende i servizi di fornitura postale e digitale; le imprese che si occupano della gestione dei rifiuti, della catena di produzione e distribuzione di sostanze chimiche o della trasformazione e distruzione di alimenti; le fabbriche di dispositivi medici; e, infine, il settore della ricerca.

c) la **gestione e la promozione e l'agevolazione al coordinamento ai fini della divulgazione delle vulnerabilità** di cui è designato il CSIRT Italia ai sensi dell'**articolo 16** dello schema di decreto in commento a cui si rimanda per un approfondimento.

Tuttavia, si ritiene opportuno ricordare anche in questa sede che il CSIRT – *Computer Emergency Response Team* – è definito dalla direttiva 2016/1148 quale "gruppo di intervento per la sicurezza informatica in caso di incidente" che ogni Stato membro è chiamato a istituire con il compito di trattare gli incidenti e i rischi secondo una procedura definita. Il CSIRT Italia è istituito presso la Presidenza del Consiglio dall'**articolo 8 del decreto legislativo NIS** fino alla modifica intercorsa con il decreto legge n. 82 del 2021 che lo ha trasferito presso l'Agenzia per la cybersicurezza nazionale mutuandone il nome che precedentemente era CSIRT italiano. La direttiva (UE) 2022/2555, che abroga quella di cui sopra, ne replica la disciplina all'**articolo 1, paragrafo 2, lettera a).** Di conseguenza, e conformemente a tale norma, l'**articolo 11** dello schema di decreto in commento aggiorna la disciplina relativa alle competenze del CSIRT Italia.

d) il **sostegno della disponibilità generale, dell'integrità e della riservatezza** del nucleo pubblico della rete aperta;
e) **l'integrazione di tecnologie avanzate** e all'avanguardia nella gestione dei rischi per la sicurezza informatica;
f) la **promozione e lo sviluppo di attività di istruzione**, di sensibilizzazione e di ricerca in materia di sicurezza informatica, nonché **orientamenti sulle buone pratiche e sui controlli** destinati ai cittadini, ai portatori di interessi e ad altri soggetti;
g) il **sostegno agli istituti accademici e di ricerca** per la promozione e la diffusione di infrastrutture e strumenti informatici sicuri;
h) lo **sviluppo di procedure adeguate per favorire la condivisione di informazioni** tra soggetti nel rispetto del diritto dell'Unione Europea;
i) il **rafforzamento dei valori di riferimento relativi alla resilienza e all'igiene informatica** delle piccole e medie imprese, in particolare per fornire a quelle escluse dall'ambito di applicazione della disposizione in commento orientamenti a sostegno dell'accessibilità;
j) la **promozione di una protezione informatica attiva**.

Il **comma 4**, infine, precisa che fatte salve le funzioni del Presidente del Consiglio previste dai **commi 1 e 2 dell'articolo 2 del decreto legge n. 82 del 2021**[6] è aggiunta alle funzione dell'Agenzia per la cybersicurezza

[6] Che si ricorda essere, in particolare, la sua titolarità, in via esclusiva, dell'alta direzione e della responsabilità generale delle politiche di cybersicurezza e, come già visto, dell'adozione della strategia nazionale una volta sentito il CIC. Ai fini dell'esercizio di tali competenze e dell'attuazione della Strategia, il Presidente del Consiglio dei ministri, sempre sentito il CIC,

nazionale, che sono elencate all'**articolo 7** del medesimo decreto legge, il compito di valutare periodicamente e aggiornare ove necessario e comunque **almeno ogni cinque anni** la Strategia sentite le amministrazioni componenti il Nucleo per la cybersicurezza e sulla base di indicatori chiave di prestazione.

Il **Nucleo per la cybersicurezza**, istituito presso l'Agenzia nazionale per la cybersicurezza dall'**articolo 8 del decreto legge n. 82 del 2021**, è l'organismo 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. Riguardo alla sua composizione il Nucleo è presieduto dal direttore generale dell'Agenzia o, per sua delega, dal vice direttore generale ed è formato 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, del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri e, per gli aspetti relativi alla trattazione di informazioni classificate, è integrato da un rappresentante dell'Ufficio centrale per la segretezza.

L'Agenzia propone poi l'aggiornamento al Presidente del Consiglio che lo adotta, sempre sentito il CIC, secondo il già citato **articolo 2, primo comma, lettera b)**, del decreto legge di cui sopra.

Si segnala, infine, che attualmente l'Agenzia per la cybersicurezza nazionale ha pubblicato la Strategia nazionale di cybersicurezza per il 2022-2026 e il suo rispettivo Piano di implementazione che rappresenta il documento operativo nel quale sono indicate le 82 misure da adottare.

Precedentemente, in ottemperanza agli obblighi stabiliti dalla prima direttiva NIS erano stati pubblicati, nel 2017, il Quadro strategico nazionale e, in sua attuazione, il Piano nazionale per la protezione cibernetica e la sicurezza informatica.

impartisce le direttive per la cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale

Articolo 10
(Autorità nazionale competente e punto di contatto unico)

L'**articolo 10** individua l'Agenzia nazionale per la cybersicurezza come autorità nazionale competente e punto di contatto unico ai fini del provvedimento.

La norma richiama, al comma 1, la definizione di "autorità nazionale competente" prevista dalla direttiva oggetto di recepimento all'articolo 8, paragrafo 1 (e cioè autorità responsabili della cybersicurezza e dei compiti di vigilanza previsti dalla direttiva). La norma quindi specifica, sempre al comma 1, che in tale ruolo l'Agenzia per la cybersicurezza:

- sovrintende all'attuazione del provvedimento in esame;
- predispone i provvedimenti attuativi;
- svolge le attività di regolazione previste dal provvedimento adottando linee guida, raccomandazioni e orientamenti non vincolanti,
- individua i soggetti essenziali e i soggetti importanti ai sensi degli articoli 3 e 6 del provvedimento (cfr. *supra* le relative schede di lettura) e redige l'elenco dei soggetti essenziali di cui all'articolo 7, comma 2 (cfr. *supra* la relativa scheda di lettura);
- partecipa al gruppo di cooperazione NIS e alle altre iniziative di cooperazione stabilite in ambito di Unione europea;
- stabilisce gli obblighi di informazione che i soggetti essenziali tenuti a iscriversi nella piattaforma digitale devono fornire, ai sensi dell'articolo 7, comma 6 (cfr. *supra* la relativa scheda di lettura) nonché quelli previsti dal Capo IV (articoli da 23 a 33) in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente (cfr. *infra* le relative schede di lettura);
- svolge i compiti di vigilanza ed esecuzione di cui al Capo V (articoli da 34 a 39, cfr. *infra* le relative schede di lettura).

Il comma 2 designa l'Agenzia per la cybersicurezza nazionale come punto di contatto unico ai sensi dell'articolo 8 paragrafo 3 della direttiva oggetto di recepimento (che appunto prevede che ogni Stato membro designi un punto di contatto unico). In quanto tale l'Agenzia svolge una funzione di collegamento per garantire la cooperazione transfrontaliera con gli altri Stati membri, con la Commissione europea e con l'ENISA (Agenzia dell'Unione europea per la Cybersicurezza).

Il comma 3 autorizza, per l'attuazione dell'articolo in commento, la spesa di due milioni di euro annui a decorrere dall'anno 2025 a cui si provvede ai sensi dell'articolo 44.

Articolo 11
(Autorità di settore NIS)

L'**articolo 11,** al fine di assicurare l'efficace attuazione del presente decreto a livello settoriale, individua le Autorità di settore NIS che supportano l'Autorità nazionale competente NIS e collaborano con essa, secondo le modalità di cui all'articolo 40, comma 2, lettera c) del decreto medesimo.

In particolare, ai sensi del **comma 2** sono designate quali **Autorità di settore NIS**:

a) **la Presidenza del Consiglio dei ministri** per:

1) il settore gestione dei servizi TIC, di cui al numero 9 dell'allegato I, in collaborazione con l'Agenzia per la cybersicurezza nazionale;
2) il settore dello spazio, di cui al numero 10 dell'allegato I;
3) il settore delle pubbliche amministrazioni, di cui all'articolo 3, commi 6 e 7;
4) le società in house e le società partecipate o a controllo pubblico, di cui al numero 4 dell'allegato IV;

b) **il Ministero dell'economia e delle finanze**, per i settori bancario e delle infrastrutture dei mercati finanziari, di cui ai numeri 3 e 4 dell'allegato I, sentite le autorità di vigilanza di settore, Banca d'Italia e Consob;

c) **il Ministero delle imprese e del *made in Italy*** per:

1) il settore delle infrastrutture digitali, di cui al numero 8 dell'allegato I;
2) il settore dei servizi postali e di corriere, di cui al numero 1 dell'allegato II;
3) il settore della fabbricazione, produzione e distribuzione di sostanze chimiche, di cui al numero 3 dell'allegato II, sentito il Ministero della salute;
4) i sottosettori della fabbricazione di computer e prodotti di elettronica e ottica, della fabbricazione di apparecchiature elettriche e della fabbricazione di macchinari e apparecchiature n.c.a., di cui alle lettere b), c) e d) del settore fabbricazione, di cui al numero 5 dell'allegato II;
5) i sottosettori della fabbricazione di autoveicoli, rimorchi e semirimorchi, e della fabbricazione di altri mezzi di trasporto, di cui alle lettere e) e f) del settore fabbricazione, di cui al numero 5 dell'allegato II, sentito il Ministero delle infrastrutture e dei trasporti;

6) i fornitori di servizi digitali, di cui al numero 6 dell'allegato II;

d) **il Ministero dell'agricoltura, della sovranità alimentare e delle foreste** per il settore produzione, trasformazione e distribuzione di alimenti, di cui al numero 4 dell'allegato II;

e) **il Ministero dell'ambiente e della sicurezza energetica** per:
1) il settore energia, di cui al numero 1 dell'allegato I;
2) i settori:
   2.1) fornitura e distribuzione di acqua potabile, di cui al numero 6 dell'allegato I;
   2.2) acque reflue, di cui al numero 7 dell'allegato I;
   2.3) gestione rifiuti, di cui al numero 2 dell'allegato II;

f) **il Ministero delle infrastrutture e dei trasporti** per:
1) il settore trasporti, di cui al numero 2 dell'allegato I;
2) i soggetti che forniscono servizi di trasporto pubblico locale di cui al numero 1 dell'allegato IV;

g) **il Ministero dell'università e della ricerca** per il settore ricerca di cui al numero 7 dell'allegato II e per gli istituti di istruzione che svolgono attività di ricerca di cui al numero 2 dell'allegato IV, anche in accordo con le altre amministrazioni vigilanti;

h) **il Ministero della cultura** per i soggetti che svolgono attività di interesse culturale di cui al numero 3 dell'allegato IV;

i) **il Ministero della salute** per:
1) il settore sanitario, di cui al numero 5 dell'allegato I;
2) il sottosettore fabbricazione di dispositivi medici e di dispositivi medicodiagnostici in vitro, di cui alla lettera a) del settore fabbricazione, di cui al numero 5 dell'allegato II.

Le Amministrazioni di cui al comma 2, per i rispettivi settori di competenza, sono altresì designate **Autorità di settore** per i soggetti di cui all'articolo 3, commi 9 e 10 (**comma 3**).

Il **comma 3** elenca le **attribuzioni delle Autorità di settore NIS** stabilendo che esse, per i rispettivi settori di competenza ai fini di cui al comma 1, procedono in particolare:
a) alla verifica dell'elenco dei soggetti essenziali e dei soggetti importanti;

b) al supporto nell'individuazione dei soggetti essenziali e dei soggetti importanti ai sensi degli articoli 3 e 6, in particolare identificando i soggetti essenziali e i soggetti importanti di cui ai commi 8, 9 e 10 dell'articolo 3;
c) all'individuazione dei soggetti a cui si applicano le deroghe di cui all'articolo 3, comma 4;
d) al supporto per le funzioni e le attività di regolamentazione di cui al presente decreto secondo le modalità di cui all'articolo 40;
e) all'elaborazione dei contributi per la relazione annuale sull'attuazione del presente decreto di cui all'articolo 12, comma 5;
f) all'istituzione e al coordinamento dei tavoli settoriali, al fine di contribuire all'efficace e coerente attuazione settoriale del presente decreto nonché al relativo monitoraggio (si precisa che per la partecipazione ai tavoli settoriali non sono previsti gettoni di presenza, compensi, rimborsi di spese o emolumenti comunque denominati);
g) alla partecipazione alle attività settoriali del Gruppo di Cooperazione NIS nonché dei consessi e delle iniziative a livello di Unione europea relativi all'attuazione della direttiva (UE) 2022/2555.

Al **comma 5** si stabilisce che, quando il soggetto critico ha carattere regionale ovvero opera esclusivamente sul territorio di una regione nei settori di cui al comma 2, lettere a), numeri 3 e 4, d), e), f), h) e i), numero 1, le modalità di **collaborazione tra le Autorità di settore e le regioni interessate** sono stabilite con **accordo** da definirsi entro il 30 settembre 2024 **in sede di Conferenza Stato-regioni**.

Per l'esercizio delle competenze attribuite dal presente decreto, al comma 6 si autorizza ciascuna autorità di settore, ad eccezione di quella indicata al comma 2, lettera b), **a reclutare** con **contratto di lavoro subordinato a tempo indeterminato**, **due unità** di **personale non dirigenziale**, appartenente all'**area funzionari** del vigente contratto collettivo nazionale - Comparto funzioni centrali, o categorie equivalenti, mediante:

- procedure di passaggio diretto di personale tra amministrazioni pubbliche ai sensi dell'articolo 30 del decreto legislativo 30 marzo 2001, n. 165,
- scorrimento di vigenti graduatorie di concorsi pubblici
- o avvio di nuove procedure concorsuali pubbliche.

I medesimi soggetti sono autorizzati altresì ad **avvalersi di personale non dirigenziale**, ad esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche, posto in posizione:

- di comando, ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127,
- di aspettativa, distacco o fuori ruolo ovvero altro analogo istituto previsto dai rispettivi ordinamenti.

Si dispone inoltre che, all'atto del collocamento fuori ruolo e per tutta la sua durata, nella dotazione organica dell'amministrazione di provenienza sia reso indisponibile un numero di posti equivalente dal punto di vista finanziario.

Per l’attuazione di quanto disposto al comma 6 è autorizzata la spesa di 409.424 euro per l’anno 2024 e di euro 925.695 annui a decorrere dall'anno 2025, a cui si provvede ai sensi dell’articolo 44 (**comma 7**).

Articolo 12
(Tavolo per l'attuazione della disciplina NIS)

L'**articolo 12** istituisce il Tavolo permanente per l'attuazione della disciplina NIS, di cui al presente provvedimento, al fine di assicurarne l'implementazione e l'attuazione.

Si ricorda che ai sensi dell'articolo 20 della direttiva gli Stati membri provvedono affinché gli organi di gestione dei soggetti essenziali e importanti approvino le misure di gestione dei rischi di cibersicurezza adottate da tali soggetti, sovraintendano alla sua attuazione.

Il **comma 1** costituisce il Tavolo presso l'Agenzia per la cybersicurezza nazionale (ACN), mentre il **comma 2** ne stabilisce la **composizione**; ne fanno parte:

- il direttore generale dell'Agenzia per la cybersicurezza nazionale, o un suo delegato, che lo presiede;
- un rappresentante di ogni Autorità di settore NIS (*si veda l'articolo 11 del presente provvedimento*);
- due rappresentanti designati dalle regioni e province autonome in sede di Conferenza Stato-regioni.

Inoltre, ai sensi del **comma 3**, possono essere chiamati a partecipare alle riunioni:

- altri rappresentanti delle amministrazioni di riferimento delle autorità NIS in relazione alle materie oggetto di trattazione;
- rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca;
- operatori privati interessati dalle previsioni di cui al presente provvedimento.

Il **comma 4** stabilisce che il Tavolo è convocato dal presidente o su richiesta di almeno tre componenti e si riunisce almeno una volta per trimestre.

Il **comma 5** individua i compiti del Tavolo come segue:

- supportare l'Agenzia per la cybersicurezza - Autorità nazionale competente NIS nello svolgimento delle funzioni relative all'implementazione e all'attuazione del presente provvedimento, con

particolare riferimento ai compiti ad essa conferiti dall'articolo 10, comma 1, (ad eccezione dei poteri di vigilanza);
- formulare proposte e pareri per l'adozione di iniziative, linee guida o atti di indirizzo;
- predisporre una relazione annuale sull'attuazione del presente provvedimento.

Con determinazione dell'ACN, sentito il Tavolo, possono essere dettate **ulteriori disposizioni per l'organizzazione** e per il funzionamento del Tavolo, per la cui partecipazione non sono previsti gettoni di presenza, compensi, rimborsi di spese o altri emolumenti, comunque denominati (**comma 6**).

Articolo 13
(Quadro nazionale di gestione delle crisi informatiche)

L'**articolo 13** individua l'**ACN** e il **Ministero della difesa** quali **Autorità nazionali di gestione delle crisi informatiche**.
Tali enti individuano le capacità, le risorse e le procedure che possono essere impiegate in caso di **crisi**. Si demanda a uno o più D.P.C.M. – da adottarsi entro 12 mesi dalla data di entrata in vigore del provvedimento – la **definizione** del **Piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala**. Il piano è aggiornato periodicamente e, comunque, ogni tre anni.
Tale piano stabilisce:

- obiettivi e misure delle attività nazionali di preparazione;
- compiti e responsabilità delle due Autorità nazionali;
- procedure di gestione delle crisi;
- pertinenti portatori di interessi pubblici e privati;
- le procedure nazionali e gli accordi tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno e la partecipazione effettivi dell'Italia alla gestione coordinata degli incidenti e delle crisi informatiche su vasta scala a livello dell'UE.

L'**articolo 13** si compone di **4 commi** ed è volto ad istituire un quadro nazionale di gestioni delle crisi informatiche.

Nello specifico, il comma **1 individua l'Agenzia per la cybersicurezza nazionale (ACN),** con funzioni di **coordinatore**, e il **Ministero della difesa,** ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera *g)* (v. *infra*).

L'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, c.d. NIS2, dispone che se uno Stato membro designa o istituisce più di un'autorità di gestione delle crisi informatiche, esso indica **chiaramente quale di tali autorità deve fungere da coordinatore** per la gestione di incidenti e crisi di cybersicurezza su vasta scala.

Il **comma 2** dispone che le citate Autorità nazionali di gestione delle crisi informatiche individuano **le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi** ai fini del presente decreto.

Il **comma 3** demanda a uno o più decreti del Presidente del Consiglio (d.P.C.M.), su proposta dell'ACN e del Ministero della difesa, previo parere del Comitato interministeriale per la sicurezza della Repubblica (CISR), la

definizione del Piano nazionale di risposta agli incidenti e alle crisi informatiche su larga scala, che viene aggiornato **periodicamente** e, comunque, **ogni 3 anni.**

Tale D.P.C.M. deve essere adottato entro **12 mesi** dall'entrata in vigore del provvedimento in esame.

Si ricorda a tale riguardo che il Comitato interministeriale per la sicurezza della Repubblica (CISR) è stato istituito presso la Presidenza del Consiglio dei ministri dalla legge n. 124 del 2007, con funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza.

Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dai seguenti membri:

- Autorità Delegata - ove istituita;
- Ministro degli Affari Esteri;
- Ministro dell'Interno;
- Ministro della Difesa;
- Ministro della Giustizia;
- Ministro dell'Economia e delle Finanze;
- Ministro delle Imprese e del Made in Italy;
- Ministro dell'Ambiente e della Sicurezza Energetica.

Il decreto specifica altresì che la composizione del Comitato interministeriale per la sicurezza della Repubblica (CISR) è quella prevista dall'articolo 10 del decreto-legge n. 82 del 2021. In particolare, secondo tali disposizioni, in 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 delle predette 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'**ACN.** Inoltre, può essere integrato da rappresentati del Ministero della Salute, Ministero dell'Interno-Dipartimento Vigili del fuoco, del soccorso pubblico e della difesa civile, nonché altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, e di altri soggetti pubblici o privati eventualmente interessati.

Il **comma 4** definisce gli aspetti che devono essere stabiliti dal citato Piano, quali:

a) gli **obiettivi** delle misure e delle attività nazionali di preparazione;

b) i **compiti** e le **responsabilità** delle Autorità nazionali di gestione delle crisi informatiche;

c) le **procedure di gestione delle crisi informatiche**, tra cui la loro integrazione nel quadro nazionale per la gestione delle crisi che coinvolgono aspetti di cybersicurezza di cui all'articolo 10 del decreto-legge n. 82 del 2021, e i canali di scambio di informazioni;

d) le **misure nazionali di preparazione**, comprese le esercitazioni e le attività di formazione;

e) i pertinenti **portatori di interessi** del settore pubblico e privato e le infrastrutture coinvolte;

f) le **procedure nazionali** e gli **accordi** tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno e la partecipazione effettivi dell'Italia alla **gestione coordinata degli incidenti e delle crisi informatiche su vasta scala a livello dell'Unione europea.**

Articolo 14, commi 1 e 2
(Cooperazione tra autorità nazionali)

L'**articolo 14, al comma 1,** dispone che siano **assicurate la cooperazione e la collaborazione** reciproca tra ACN e l'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazioni (autorità di contrasto), il GPDP, l'Ente nazionale per l'aviazione civile, l'AgID, l'AGCOM, e il Ministero della Difesa, nonché con altre autorità nazionali competenti, per lo **scambio periodico di informazioni** pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.
Il **comma 2**, dispone che l'**ACN e GPDP** cooperino nei casi di incidenti che comportano violazioni dei **dati personali**. Inoltre, qualora il GPDP o le autorità di controllo di altri Stati membri impongano una sanzione amministrativa pecuniaria, l'ACN non procede all'irrogazione delle sanzioni amministrative pecuniarie imputabile al medesimo comportamento. Infine si prevede l'adozione di un D.P.C.M. per definire l'**elenco dei soggetti** – all'interno di quelli individuati annualmente come "essenziali" o "importanti" ai sensi del comma 2 dell'art. 7 – che impattano sulla **efficienza dello Strumento militare** e sulla **tutela della difesa** e **sicurezza militare** dello Stato, su cui l'ACN comunica tempestivamente al Ministero della difesa gli incidenti e le ulteriori informazioni di sicurezza cibernetica.

Il **comma 1** dell'articolo in commento dispone che sono assicurate la **cooperazione** e la **collaborazione reciproca dell'ACN** in quanto **A**utorità nazionale competente NIS e i seguenti organi:

- Autorità di Contrasto del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione (Autorità di contrasto);
- **Garante per la protezione dei dati personali** quale autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679;
- l'**Ente nazionale per l'aviazione civile (ENAC)** quale autorità nazionale ai sensi dei regolamenti (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, e (UE) 2018/1139, del Parlamento europeo e del Consiglio, del 4 luglio 2018;
- l'**Agenzia per l'Italia digitale (AgID)** quale organismo di vigilanza ai sensi del regolamento (UE) n. 910/2014;
- l'**Autorità per le garanzie nelle comunicazioni** quale autorità nazionale di regolamentazione ai sensi della direttiva (UE) 2018/1972;
- **Ministero della difesa**, quale responsabile in materia di difesa dello Stato;

- **Altre autorità nazionali competenti** anche ai sensi di altri atti giuridici settoriali dell'Unione europea, ivi incluso lo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.

Come riportato anche dalla relazione illustrativa, l'articolo in esame definisce le modalità di cooperazione a livello nazionale integrando le previsioni della direttiva NIS2 con quanto già disposto dall'abrogando d.lgs. n. 65 del 2018, nel rispetto dell'articolo 3, comma 1, lettera o), della legge di delegazione europea 20222023 che prevede di "assicurare il migliore coordinamento tra le disposizioni adottate ai sensi del presente articolo per il recepimento della direttiva (UE) 2022/2555, le disposizioni adottate ai sensi dell'articolo 5 della presente legge per il recepimento della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, nonché le disposizioni del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, e quelle adottate ai sensi dell'articolo 16 della presente legge per l'adeguamento a quest'ultimo e per il recepimento della direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022.

Il **comma 2** prevede, ai fini della cooperazione e collaborazione di cui al comma 1, che:

- l'**ACN coopera con il Garante per la protezione dei dati personali**, in relazione agli incidenti che comportano violazioni di dati personali, senza pregiudicare la competenza e i compiti di controllo di cui al GDPR;

Ai sensi dell'articolo 7, comma 5, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, nei casi di incidenti, l'**ACN può consultare il Garante** e **collaborare** 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.

- qualora l'**ACN, in sede di vigilanza o di esecuzione**, venga a conoscenza del fatto che la violazione degli obblighi in materia di misure di gestione dei rischi per la sicurezza informativa, di cui all'articolo 24 (v. *infra*) da parte di un soggetto essenziale o importante possa comportare una **violazione dei dati personali**, ne **informa senza indebito ritardo il Garante per la protezione dei dati personali**;

Il GDPR, all'articolo 4, punto 12), definisce la "**violazione dei dati personali**", come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". Si ricorda altresì che tale

violazione deve essere notificata altresì ai sensi dell'articolo 33 del medesimo regolamento.

- qualora il **Garante per la protezione dei dati personali o le autorità di controllo di altri Stati membri** impongano una sanzione amministrativa pecuniaria ai sensi del GDPR, l'ACN non procede all'irrogazione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 38 (v. *infra*), per una violazione dei dati personali, di cui sopra, imputabile al **medesimo comportamento**. L'ACN può tuttavia esercitare i **poteri di esecuzione**, di cui all'articolo 37 del presente provvedimento (v. *infra*)
- l'adozione di un D.P.C.M., su proposta del Ministro della difesa, sentita l'ACN, per definire l'**elenco dei soggetti** – all'interno di quelli individuati annualmente come "essenziali" o "importanti" (v. *infra*) – che impattano sulla **efficienza dello Strumento militare** e sulla **tutela della difesa** e **sicurezza militare** dello Stato, su cui l'ACN comunica tempestivamente al Ministero della difesa gli incidenti di cui all'articolo 25 (v. *infra*) e le ulteriori informazioni di sicurezza cibernetica.

Articolo 14, commi 3 - 6
(Cooperazione tra autorità nazionali)

Il **comma 3 dell'articolo 14**, specifica che la collaborazione tra l'ACN e le altre autorità nazionali sia assicurata con gli strumenti previsti dal regolamento cosiddetto DORA e dal provvedimento di attuazione.
Il **comma 4** specifica che l'ACN **informa il forum di sorveglianza** quando esercita i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli **obblighi** previsti dal provvedimento da parte di un **soggetto essenziale designato come fornitore terzo critico di servizi di ICT.**
Il **comma 5** specifica che l'ACN coopera con le autorità nazionali competenti anche con lo scambio periodico di informazioni riguardo all'**identificazione di soggetti critici, sui rischi, sulle minacce e sugli incidenti sia informatici che non informatici** che interessano i soggetti identificati come critici, e sulle misure adottate in risposta a tali rischi, minacce e incidenti.
Il **comma 6** disciplina le modalità esecutive per la collaborazione di cui al comma precedente.

Il **comma 3** dell'articolo in esame, dispone che la cooperazione e la collaborazione reciproca dell'ACN e delle autorità nazionali competenti sia assicurata dall'ACN con le autorità nazionali competenti di cui al è assicurata con gli strumenti di cui al c.d. **Regolamento DORA** (*Digital Operational Resilience Act*), e alla disciplina nazionale di attuazione, in relazione, tra l'altro, allo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.

Il **Regolamento (UE) 2022/2554,** cosiddetto **DORA**, pubblicato nella Gazzetta Ufficiale dell'Unione Europea del 27 dicembre 2022, definisce obblighi sulla **sicurezza dei sistemi informatici e di rete** che he sostengono i processi commerciali delle entità finanziarie, riunendo per la prima volta in un unico atto legislativo tutte le disposizioni in materia di rischio digitale nel settore finanziario.

Si ricorda, a tal proposito, che il citato regolamento, così come la direttiva NIS2, fanno parte di un più ampio pacchetto di **strumenti giuridici a livello dell'Unione,** mirato a rafforzare i soggetti pubblici e privati rispetto alle minacce nell'ambito cibernetico. In particolare, oltre ai citati atti, vi sono:

- la **direttiva (UE) 2022/2557 (cosiddetta direttiva CER – *Critical Entities Resilience*)**, relativa alla resilienza dei soggetti critici e interviene in abrogazione della precedente direttiva 2008/114/CE del Consiglio, concernente l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione;

- la **direttiva (UE) 2022/2556**, correlata al **Regolamento DORA,** che reca una serie di modifiche necessarie per rendere chiara e coerente l'applicazione, da parte delle entità finanziarie autorizzate e sottoposte a vigilanza conformemente a tali direttive, dei vari requisiti di resilienza operativa digitale necessari per lo svolgimento delle loro attività e per la prestazione di servizi.

La legge n. 15/2024, c.d. "**Legge di delegazione europea 2022-2023**", all'articolo 3 relativo al recepimento della Direttiva NIS2, dispone in tal senso che sia assicurato, tra le altre cose, il **coordinamento** delle disposizioni recanti il recepimento della direttiva NIS2 con il **regolamento (UE) 2022/2554**, ivi comprese le disposizioni nazionali di adeguamento a quest'ultimo.

Inoltre, all'articolo 16 della citata legge sono contenuti i principi e criteri direttivi per l'adeguamento della normativa nazionale alle disposizioni del regolamento DORA e la direttiva ad esso collegata. In particolare, elenca i seguenti **principi e criteri direttivi specifici** per l'esercizio della delega:

a. apportare alla normativa vigente le occorrenti modifiche e integrazioni, anche al sistema sanzionatorio, necessarie all'**adeguamento dell'ordinamento giuridico nazionale** al regolamento (UE) 2022/2554 e al recepimento della direttiva (UE) 2022/2556, incluso l'**eventuale esercizio delle opzioni**, anche mediante la normativa secondaria di cui alla lettera d), previste dal regolamento (UE) 2022/2554. Nell'adozione di tali modifiche e integrazioni il Governo tiene conto degli **orientamenti delle Autorità di vigilanza europee**, degli **atti delegati adottati dalla Commissione europea** e delle disposizioni legislative nazionali di **recepimento delle seguenti direttive** strettamente correlate al regolamento (UE) 2022/2554:
    1. la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a **misure per un livello comune elevato di cybersicurezza nell'Unione**, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2);
    2. la direttiva (UE) 2022/2557 del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla **resilienza dei soggetti critici** e che abroga la direttiva 2008/114/CE del Consiglio;
b. assicurare che alle **autorità competenti**, individuate ai sensi dell'articolo 19, comma 1, paragrafo 2, e dell'articolo 46 del regolamento (UE) 2022/2554, siano attribuiti tutti i **poteri di vigilanza, di indagine e sanzionatori** per l'attuazione del regolamento (UE) 2022/2554 e della direttiva (UE) 2022/2556, coerentemente con il riparto di competenze nel settore finanziario nazionale;
c. attribuire alle autorità di cui alla lettera b) il potere di imporre le **sanzioni e le altre misure amministrative** previste dagli articoli 42, paragrafo 6, e 50 del regolamento (UE) 2022/2554, nel rispetto dei limiti edittali e delle procedure previsti dalle disposizioni nazionali che disciplinano l'irrogazione delle sanzioni e l'applicazione delle altre misure

amministrative da parte delle autorità anzidette, avuto riguardo al riparto di competenze nel settore finanziario nazionale;

d. prevedere, ove opportuno, il ricorso alla **disciplina secondaria adottata dalle autorità** indicate alla lettera b) secondo le rispettive competenze.

(Per ulteriori approfondimenti si rimanda al relativo *dossier*)

Il **comma 4** specifica che l'ACN cooperi con le autorità nazionali competenti degli altri stati, di cui al regolamento DORA, informando, in particolare il **forum di sorveglianza** quando esercita i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dal presente decreto da parte di un soggetto essenziale o importante designato come fornitore terzo critico di servizi di ICT, individuato ai sensi dell'articolo 31 del regolamento DORA.

Il forum di sorveglianza è istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento DORA, che introduce un quadro di sorveglianza specifico per la vigilanza dei fornitori di servizi ICT di terze parti designati come critici. In questo contesto, il forum di sorveglianza è istituito al fine di discutere i pertinenti sviluppi in materia di rischi e vulnerabilità relativi all'ICT e **promuovere un approccio coerente al monitoraggio** a livello dell'Unione; valutare, con cadenza annuale, le attività di sorveglianza, promuovere le misure per aumentare la resilienza operativa digitale e favorire le migliori pratiche. Si devono poi sottoporre **parametri di riferimento generali** per i fornitori di servizi ICT critici.

Il **comma 5** dell'articolo in esame, dispone la cooperazione e la collaborazione tra l'ACN e le autorità nazionale competenti, di cui alla direttiva (UE) 2022/2557 relativa alla **resilienza dei soggetti critici**, anche con lo scambio periodico di informazioni riguardo:

- all'identificazione di soggetti critici,
- sui rischi, sulle minacce e sugli incidenti sia informatici che non informatici che interessano i soggetti identificati come critici ai sensi della citata direttiva;
- sulle misure adottate in risposta a tali rischi, minacce e incidenti.

In particolare, la citata direttiva prescrive (all'articolo 9) agli Stati membri di designare o istituire una o più **autorità competenti responsabili della sua corretta applicazione ed esecuzione,** nonché un punto di contatto unico, a fini di cooperazione transfrontaliera e di scambio di informazioni.

Lo schema di decreto legislativo recante attuazione della direttiva, designa, all'articolo 5, le **Autorità settoriali competenti**, responsabili dell'applicazione e dell'esecuzione dell'atto di recepimento della direttiva europea.

Esse sono, va da sé, diversificate a seconda dei settori di attività considerati come suscettibili di servizi essenziali, e sono:

- Ministero dell'ambiente e della sicurezza energetica, per il settore: ENERGIA, sottosettori: energia elettrica; teleriscaldamento e tele-raffrescamento; petrolio; gas; idrogeno;
- Ministero delle infrastrutture e dei trasporti, per il settore: TRASPORTI, sottosettori: trasporto aereo; trasporto ferroviario; trasporto per vie d'acqua; trasporto su strada; trasporto pubblico; e per il settore: ACQUE IRRIGUE (quest'ultimo, non ricompreso nell'elenco dei settori della direttiva n. 2557 né dal regolamento delegato integrativo n. 2450 del 2023, è presente nell'allegato A in calce allo schema, avvalendosi di facoltà integrativa attribuita dalla norma di delega);
- Ministero dell'economia e delle finanze, per il settore: BANCARIO, e per il settore: INFRASTRUTTURE DEI MERCATI FINANZIARI. Peraltro è prevista la collaborazione con le autorità di vigilanza di settore, la Banca d'Italia, la Commissione nazionale per la società e la borsa (Consob);
- Ministero della salute, direttamente o per il tramite delle proprie autorità territoriali, e, per gli ambiti di propria competenza, l'Agenzia italiana del farmaco (AIFA), per il settore: SALUTE;
- Ministero dell'ambiente e della sicurezza energetica, direttamente o per il tramite delle proprie autorità territoriali, per il settore: ACQUA POTABILE, e per il settore: ACQUE REFLUE;
- Agenzia per la cybersicurezza nazionale, per il settore: INFRASTRUTTURE DIGITALI, in collaborazione con il Ministero delle imprese e del *made in Italy*, per le attività di valutazione del rischio e di individuazione dei soggetti critici (cfr. articoli 7 e 8 dello schema);
- Presidenza del Consiglio dei ministri, per il settore: SPAZIO;
- Ministero dell'agricoltura, della sovranità alimentare e delle foreste, per il settore: produzione, trasformazione e distribuzione di ALIMENTI.
- i diversi Ministeri sopra ricordati, negli ambiti di propria competenza, ovvero la Presidenza del Consiglio, per gli enti individuati con apposito D.P.C.M. da adottarsi entro il 17 gennaio 2026, per il settore: ENTI DELLA PUBBLICA AMMINISTRAZIONE.

(Per maggiori approfondimenti si rimanda al relativo *dossier*)

Il **comma 6** dell'articolo in esame prevede che ai fini della cooperazione e della collaborazione di cui al comma 5:

- il punto di contatto unico e le autorità competenti di cui al decreto legislativo comunicano tempestivamente all'ACN i soggetti identificati come soggetti critici ai sensi del decreto legislativo di recepimento della direttiva (UE) 2022/2557, relativa alla **resilienza dei soggetti critici**, e successivi aggiornamenti;
- le autorità nazionali competenti ai sensi del decreto legislativo di recepimento della citata direttiva possono chiedere all'ACN di

svolgere le attività ed esercitare i poteri di cui al capo V in relazione a un soggetto che è stato individuato come soggetto critico ai sensi del citato decreto legislativo (v. *infra*).

Articolo 15
(Gruppo nazionale di risposta agli incidenti di sicurezza informatica – CSIRT Italia)

L'**articolo 15** si compone di **8 commi** e reca le **funzioni**, le **dotazioni**, i **compiti** e le forme di **collaborazione** del **gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT Italia)**.

Il CSIRT Italia è istituito presso l'Agenzia per la cybersicurezza nazionale (ACN). I compiti del CSIRT sono definiti dal D.Lgs n. 65 del 2018 e dal D.P.C.M. n. 4 del 2019. Essi includono:

- il monitoraggio degli incidenti a livello nazionale;
- l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti;
- l'intervento in caso di incidente;
- l'analisi dinamica dei rischi e degli incidenti;
- la sensibilizzazione situazionale;
- la partecipazione alla rete dei CSIRT.

Il CSIRT stabilisce relazioni di cooperazione con il settore privato. Inoltre, per facilitare la cooperazione, il CSIRT promuove l'adozione e l'uso di prassi comuni o standardizzate nei settori delle procedure di trattamento degli incidenti e dei rischi e sistemi di classificazione degli incidenti, dei rischi e delle informazioni.

Come ricordato anche nella relazione illustrativa, l'articolo in esame disciplina i Gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) **integrando le previsioni della direttiva NIS2** con quanto **già disposto dall'abrogando d.lgs. n. 65 del 2018,** nel rispetto dell'articolo 3, comma 1, lettera e), della legge di delegazione europea 2022-2023 che prevede "in relazione all'istituzione del team di risposta agli incidenti di sicurezza informatica (CSIRT), di cui all'articolo 10 della direttiva (UE) 2022/2555, di **confermare le disposizioni** dell'articolo 8 del decreto legislativo 18 maggio 2018, n. 65, in materia di istituzione del CSIRT Italia, nonché **ampliare** quanto previsto dal medesimo decreto legislativo prevedendo la collaborazione tra tutte le strutture pubbliche con funzioni di **Computer Emergency Response Team (CERT)** coinvolte in caso di eventi malevoli per la sicurezza informatica".

Il **comma 1** dell'articolo in esame reca le seguenti disposizioni relative al CSIRT Italia, fermo restando quanto previsto dal decreto-legge n. 82 del 2021, convertito, con modificazioni, dalla legge n. 109 del 2021, relativo all'istituzione e i compiti dell'ACN:

a) è l'organo preposto alle funzioni di **gestione degli incidenti di sicurezza informatica** per i settori, i sottosettori e le tipologie di

soggetti di cui agli allegati I, II, III e IV, conformemente a modalità e procedure definite dal CSIRT stesso;

b) dispone di un'**infrastruttura di informazione e comunicazione appropriata, sicura** e **resiliente** a livello nazionale attraverso la quale scambiare informazioni con i soggetti essenziali o importanti e con gli altri portatori di interesse pertinenti;
c) **coopera** e, se opportuno, scambia informazioni pertinenti conformemente all'articolo 17 (v. *infra*) con comunità settoriali o intersettoriali di soggetti essenziali e di soggetti importanti;
d) partecipa alla **revisione tra pari** di cui all'articolo 21 (v. *infra*);
e) garantisce la **collaborazione** effettiva, efficiente e sicura, nella Rete di CSIRT nazionali di cui all'articolo 20 (v. *infra*);
f) può stabilire **relazioni di cooperazione** con gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi. Nell'ambito di tali relazioni di cooperazione, facilita uno s**cambio di informazioni efficace, efficiente e sicuro** con tali CSIRT nazionali, o strutture nazionali equivalenti di Paesi terzi, utilizzando i pertinenti protocolli di condivisione delle informazioni, ivi inclusi quelli adottati e sviluppati dalle principali comunità nazionali, europee e internazionali del settore. Il CSIRT Italia può scambiare informazioni pertinenti con Gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi o con organismi equivalenti di Paesi terzi, compresi dati personali ai sensi della normativa nazionale vigente e del diritto dell'Unione europea in materia di protezione dei dati personali;
g) può c**ooperare con Gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi** o con organismi equivalenti di Paesi terzi, in particolare al fine di fornire loro **assistenza** in materia di sicurezza informatica.

Tali forme di cooperazione sono disciplinate, come riportato anche dall'articolato del presente provvedimento, ai sensi dell'articolo 7, comma 1, lettera s), del decreto-legge n. 82 del 2021, convertito con modificazioni dalla legge n. 109 del 2021. Secondo tali disposizioni, l'ACN può stipulare **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.

Il **comma 2** dell'articolo in esame, prevede le seguenti dotazioni del CSIRT Italia:

- è dotato di un alto livello di **disponibilità dei propri canali di comunicazione** evitando singoli punti di malfunzionamento e dispone di mezzi che gli permettono di essere contattato e di contattare i soggetti e altri CSIRT nazionali in qualsiasi momento. Il CSIRT Italia indica chiaramente i canali di comunicazione e li rende noti ai soggetti e agli altri CSIRT nazionali;
- dispone di **locali e sistemi informativi di supporto ubicati in siti sicuri**;
- utilizza un sistema adeguato di **gestione** e **inoltro** delle **richieste**, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;
- garantisce la **riservatezza** e **l'affidabilità** delle proprie attività;
- è dotato di sistemi **ridondanti** e spazi di **lavoro di backup** al fine di garantire la continuità dei propri servizi;
- partecipa, se del caso, a reti di cooperazione internazionale.

Il **comma 3** individua i seguenti **compiti** del CSIRT Italia:

- **monitora e analizza le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale** e, su richiesta, fornisce assistenza ai soggetti essenziali e ai soggetti importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informativi e di rete, secondo un ordine di priorità delle attività definito dal CSIRT Italia, onde evitare oneri sproporzionati o eccessivi;
- **emette preallarmi, allerte e bollettini** e **divulga informazion**i ai soggetti essenziali e ai soggetti importanti interessati, nonché alle autorità nazionali competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale;
- fornisce una **risposta agli incidenti** e **assistenza** ai soggetti essenziali e ai soggetti importanti interessati, ove possibile;
- **raccoglie e analizza dati forensi** e fornisce un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla sicurezza informatica;
- effettua, su richiesta di un soggetto essenziale o importante, secondo modalità e procedure definite, una s**cansione proattiva dei sistemi informativi e di rete** del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo;

- partecipa alla **Rete di CSIRT nazionali** di cui all'articolo 20 (v. *infra*) e fornisce assistenza reciproca secondo le proprie capacità e competenze agli altri membri della Rete di CSIRT nazionali su loro richiesta;
- agisce in qualità di **coordinatore** ai fini del processo di **divulgazione coordinata delle vulnerabilità** di cui all'articolo 16 (v. *infra*);
- contribuisce allo sviluppo di **strumenti sicuri** per la condivisione delle informazioni di cui al comma 1, lettera b);
- può effettuare, secondo modalità e procedure definite, una **scansione proattiva e non intrusiva dei sistemi informativi e di rete** accessibili al pubblico di soggetti essenziali e di soggetti importanti. Tale scansione è effettuata per individuare sistemi informativi e di rete vulnerabili o configurati in modo non sicuro e per informare i soggetti interessati. Tale scansione non ha alcun impatto negativo sul funzionamento dei servizi dei soggetti.

Il **comma 4** dispone che il CSIRT Italia applichi un **approccio basato sul rischio** per stabilire l'ordine di priorità nello svolgimento dei suddetti compiti di cui al comma 3.

Il **comma 5** prevede che in caso di **eventi malevoli** per la sicurezza informatica, le strutture pubbliche con funzione di ***computer emergency response team*** **(CERT) collaborano con il CSIRT Italia**, anche ai fini di un più efficace coordinamento della risposta agli incidenti.

Un CERT è un'organizzazione che raccoglie le segnalazioni di incidenti informatici e potenziali vulnerabilità dei software e produce periodicamente un bollettino sulla sicurezza informatica per informazione aziende, enti e privati cittadini delle problematiche emerse.

Sempre in ambito di collaborazione, il **comma 6** dispone che il CSIRT Italia instaura **rapporti di cooperazione** con i pertinenti portatori di interesse nazionali del **settore privato** al fine di perseguire gli obiettivi del presente decreto in relazione alle proprie competenze.

Il **comma 7**, dispone che al fine di agevolare la collaborazione con i CERT, il CSIRT Italia promuove l'**adozione e l'uso di pratiche, sistemi di classificazione e tassonomia standardizzati o comuni** per quanto riguarda:

a) le procedure di gestione degli incidenti;

b) la divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 16 (v. *infra*)

Il **comma 8**, infine, autorizza ai fini del presente articolo la spesa pari a **euro 2.000.000 annui a decorrere dall'anno 2025,** a cui si provvede ai sensi dell'articolo 44 (v. *infra*).

Articolo 16
(Divulgazione coordinata delle vulnerabilità)

L'**articolo 16** attribuisce **gruppo nazionale di risposta agli incidenti di sicurezza informatica (CSIRT Italia)** il ruolo di **coordinatore** dei soggetti interessati ai fini della divulgazione coordinata delle vulnerabilità. e di **intermediario** tra la persona fisica o giuridica che segnala la vulnerabilità e il fabbricante o fornitore di servizi TIC o prodotti TIC potenzialmente vulnerabili, su richiesta di una delle parti, prevedendo che sia adottata da parte dell'Autorità nazionale competente NIS una **politica nazionale di divulgazione coordinata delle vulnerabilità**, tenuto conto degli orientamenti del gruppo di cooperazione NIS.

In premessa si ricorda che la **divulgazione coordinata delle vulnerabilità** consiste in un processo strutturato attraverso il quale le vulnerabilità nei sistemi informatici e di rete sono segnalate al fabbricante o al fornitore dei prodotti TIC o dei servizi TIC potenzialmente vulnerabili, in modo tale da consentire loro di diagnosticarle ed eliminarle prima che informazioni dettagliate in merito siano divulgate a terzi o al pubblico. A tale riguardo, le norme internazionali ISO/IEC 30111 e ISO/IEC 29147 forniscono orientamenti sulla gestione delle vulnerabilità e sulla divulgazione delle vulnerabilità. La direttiva NIS 2, al fine di facilitare il contesto della divulgazione volontaria delle vulnerabilità, richiede agli stati membri di:

- designare uno dei loro CSIRT per coordinare la divulgazione delle vulnerabilità individuate nei prodotti o servizi TIC, stabilendo una politica nazionale coerente; e
- fare in modo che le persone negli Stati membri siano in grado di segnalare vulnerabilità in forma anonima, qualora lo richiedano.

La direttiva (considerando n. 60) richiama come nell'ambito di tale politica nazionale, gli Stati membri dovrebbero mirare ad affrontare, nella misura del possibile, le sfide incontrate dagli esperti che fanno ricerca sulle vulnerabilità, compresa la loro potenziale esposizione alla responsabilità penale, conformemente al diritto nazionale. Dato che in alcuni Stati membri le persone fisiche e giuridiche che fanno ricerca sulle vulnerabilità potrebbero essere esposte alla responsabilità penale e civile, gli Stati membri sono incoraggiati ad adottare linee guida per quanto riguarda la non perseguibilità dei ricercatori in materia di sicurezza delle informazioni e l'esenzione dalla responsabilità civile per le loro attività.

Contestualmente la direttiva inoltre prevede che l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) istituirà e manterrà una **banca dati europea delle vulnerabilità**, che contiene: a) informazioni che illustrano la vulnerabilità; b) i

prodotti o servizi TIC interessati e la gravità della vulnerabilità; c) la disponibilità di relative patch e, qualora queste non fossero disponibili, gli orientamenti forniti dalle autorità nazionali competenti o dai CSIRT rivolti agli utenti dei prodotti TIC e dei servizi TIC vulnerabili sulle possibili modalità di attenuazione dei rischi.

A tale fine i **commi 1-3** della disposizione riprendono quanto prescritto ai sensi dell'**articolo 12, co. 1, della direttiva NIS2** attribuendo al CSIRT Italia, in veste di coordinatore, i seguenti compiti:

a) l'individuazione e il contatto dei soggetti interessati;
b) l'assistenza alle persone fisiche o giuridiche che segnalano una vulnerabilità;
c) la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità che interessano più soggetti.

Si prevede inoltre che le persone fisiche o giuridiche possano fare **segnalazioni in forma anonima**, qualora lo richiedano, una vulnerabilità al CSIRT Italia, che, in veste di coordinatore, dovrà garantire un seguito alla segnalazione e assicurare l'anonimato del segnalante. Il CSIRT Italia coopera, ove opportuno, con altri CSIRT designati in qualità di coordinatori nei casi in cui la segnalazione sia suscettibile di avere un impatto significativo su soggetti in più di uno Stato membro.

Infine, l'articolo 16 assegna all'Agenzia per la cybersicurezza nazionale in compito di adottare, con una o più determinazioni, sentito il Tavolo per l'attuazione della disciplina NIS, una **politica nazionale di divulgazione coordinata** delle vulnerabilità, nonché di **implementare mezzi tecnici** per agevolare l'attuazione di tale politica (comma 4).

Articolo 17
(Accordi di condivisione delle informazioni sulla sicurezza informatica)

L'**articolo 17** disciplina lo scambio volontario di informazioni sulla sicurezza informatica tra i soggetti coinvolti. Questi scambi possono riguardare minacce informatiche, vulnerabilità e raccomandazioni, e sono finalizzati a prevenire incidenti e migliorare la sicurezza informatica.
Lo scambio di informazioni avviene tra soggetti essenziali, soggetti importanti e, se opportuno, relativi fornitori, tramite accordi specifici che rispettano la natura sensibile delle informazioni. L'Agenzia per la cybersicurezza nazionale facilita questi accordi, definendo anche gli elementi operativi e supportando i soggetti coinvolti.
I soggetti essenziali e i soggetti importanti devono notificare la loro partecipazione o ritiro dagli accordi. Gli Organismi di informazione per la sicurezza hanno accesso alle informazioni rilevanti.

L'articolo 17 consta di cinque commi e recepisce l'articolo 29 della direttiva 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022.

Il **comma 1** stabilisce che i soggetti rientranti nell'ambito di applicazione del decreto (si rinvia, sul punto, alla scheda dell'articolo 3) e, se opportuno, altri soggetti, possono volontariamente scambiarsi informazioni riguardanti la sicurezza informatica, quali minacce informatiche, quasi-incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di sicurezza informatica e raccomandazioni per la configurazione degli strumenti di sicurezza informatica atti ad individuare le minacce informatiche.

Si ricorda che ai sensi dell'articolo 2 del decreto in commento:

- per "**sicurezza informatica**" si intende l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche;
- per "**minaccia informatica**" si intende qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone;
- per "**incidente**" si intende un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o

elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi;

- per "**quasi incidente**" si intende un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato;
- per "**vulnerabilità**" si intende un punto debole, una suscettibilità o un difetto di prodotti TIC (un elemento o un gruppo di elementi di un sistema informativo o di rete) o servizi TIC (un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo dei sistemi informativi e di rete) che può essere sfruttato da una minaccia informatica.

Lo scambio di informazioni anzidetto è possibile allorquando:

a) abbia l'obiettivo di prevenire o rilevare gli incidenti, nonché di recuperare o mitigarne l'impatto;
b) aumenti il livello di sicurezza informatica, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento, contenimento e prevenzione delle minacce, strategie di mitigazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati.

Il **comma 2** stabilisce che lo scambio di informazioni avvenga nell'ambito di comunità di soggetti essenziali e di soggetti importanti e, se opportuno, dei loro fornitori o fornitori di servizi.

Nel rinviare alla scheda dell'articolo 6 per approfondimenti, si ricorda che sono "**soggetti essenziali**":

- i soggetti operanti nei settori ad alta criticità indicati nell'allegato I che superano i massimali per le medie imprese (occupanti più di 249 persone e il cui fatturato annuo superi i 50 milioni di euro oppure il cui totale di bilancio annuo superi i 43 milioni di euro);
- i soggetti identificati come "soggetti critici" ai sensi del decreto legislativo, attualmente all'esame delle Camere (A.G. 165), che recepisce la direttiva (UE) 2022/2557, indipendentemente dalle loro dimensioni;
- i fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico aventi i requisiti dimensionali delle medie imprese;
- i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, indipendentemente dalle loro dimensioni;

- pubbliche amministrazioni centrali, indipendentemente dalle loro dimensioni (Organi costituzionali e di rilievo costituzionale, Presidenza del Consiglio dei ministri e Ministeri, Agenzie fiscali e Autorità amministrative indipendenti);
- i soggetti, indipendentemente dalle loro dimensioni, individuati dall'Autorità nazionale competente NIS nell'ambito: delle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III; dei soggetti delle tipologie di cui all'allegato IV (soggetti che forniscono servizi di trasporto pubblico locale, istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, società *in house*, società partecipate e società a controllo pubblico, come definite nel D.Lgs. n. 175/2016; dei soggetti delle tipologie di cui agli allegati I (settori ad alta criticità), II (settori critici) e IV (ulteriori tipologie di soggetti), indipendentemente dalle loro dimensioni, laddove soddisfino determinati requisiti; le imprese collegate ad un soggetto essenziale o importante, se soddisfa determinati requisiti (art. 3, co. 10).

Sono "**soggetti importanti**" tutti i soggetti pubblici e privati che rientrano nell'ambito di applicazione del decreto (articolo 3) e che non sono considerati essenziali.

Lo scambio di informazioni è attuato mediante accordi di condivisione delle informazioni sulla sicurezza informatica che tengono conto della natura potenzialmente sensibile delle informazioni condivise.

Il **comma 3** pone alcuni poteri in capo all'Agenzia per la cybersicurezza nazionale.

Si tratta di un'agenzia istituita dal comma 1 dell'articolo 5 del decreto-legge 82 del 2021. L'Agenzia, a norma dell'articolo 10 del presente decreto, è Autorità nazionale competente NIS (si rinvia alla scheda dell'articolo 10 per approfondimenti).

Per effetto del **primo periodo** della disposizione in commento, l'Agenzia, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia (Gruppo nazionale di risposta agli incidenti di sicurezza informatica), favorisce la conclusione degli accordi di condivisione delle informazioni sulla sicurezza informatica e può specificare gli elementi operativi, compreso l'uso di piattaforme TIC dedicate e di strumenti di automazione, i contenuti e le condizioni degli accordi di condivisione delle informazioni. Nell'operare in tal senso, l'Agenzia tiene conto degli orientamenti e delle migliori pratiche non vincolanti elaborati da dall'Agenzia dell'Unione europea per la sicurezza informatica (Enisa).

Il **secondo periodo** del comma 3 prevede che l'Autorità nazionale competente NIS (Agenzia per la cybersicurezza nazionale), nello stabilire i dettagli relativi alla partecipazione delle autorità pubbliche agli accordi di

condivisione delle informazioni, sentito il Tavolo per l'attuazione della disciplina NIS (disciplinato dall'articolo 12 del provvedimento in commento), possa imporre condizioni per le informazioni messe a disposizione dalle autorità competenti e dal CSIRT Italia.

Il **terzo periodo** prevede che, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, l'Agenzia per la cybersicurezza nazionale supporti i soggetti essenziali e i soggetti importanti per l'applicazione degli accordi di condivisione delle informazioni sulla sicurezza informatica, conformemente alle loro misure strategiche di cui all'articolo 9, comma 3, lettera h) (messa a punto di procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni sulla sicurezza informatica tra soggetti, nel rispetto del diritto dell'Unione europea).

Il **comma 4** pone in capo ai soggetti essenziali e ai soggetti importanti un obbligo di notifica nei confronti dell'Autorità nazionale competente NIS (Agenzia nazionale per la cybersicurezza). Tale notifica avviene in occasione della partecipazione dei soggetti anzidetti agli accordi di condivisione delle informazioni sulla sicurezza informatica e, precisamente, al momento della conclusione di tali accordi o, ove applicabile, del ritiro degli stessi soggetti da tali accordi, una volta divenuto effettivo.

Per effetto del **comma 5**, gli Organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007 hanno accesso a determinate informazioni rilevanti.

Si ricorda che la legge n. 124 del 2007 dispone in merito al Sistema di informazione per la sicurezza della Repubblica e reca una nuova disciplina del segreto. All'articolo 4 è disciplinato il **Dipartimento delle informazioni per la sicurezza**. Esso è istituito presso la Presidenza del Consiglio dei ministri e, tra i numerosi compiti: coordina l'intera attività di informazione per la sicurezza; trasmette al Presidente del Consiglio dei ministri le informative e le analisi prodotte da tutto il Sistema di informazione per la sicurezza; raccoglie le informazioni provenienti dai servizi di informazione per la sicurezza, dalle Forze armate e di polizia, dalle amministrazioni dello Stato e da enti di ricerca anche privati. Gli articoli 6 e 7 della legge anzidetta disciplinano rispettivamente **l'Agenzia informazione e sicurezza esterna** e **l'Agenzia informazioni e sicurezza interna**. Le Agenzie citate effettuano il concreto compito di ricerca ed elaborazione delle informazioni utili alla sicurezza della Repubblica.

Le informazioni alle quali deve essere assicurato l'accesso agli Organismi di informazione per la sicurezza citati riguardano:

- l’elenco dei soggetti essenziali e dei soggetti importanti, tramite la piattaforma digitale di cui all’articolo 7 utilizzata per l’identificazione e l’elencazione dei soggetti essenziali e dei soggetti importanti;
- le notifiche di cui agli articoli 25 e 26 relative, rispettivamente, agli obblighi in materia di notifica di incidente e alle notifiche volontarie di informazioni pertinenti;
- le vulnerabilità rilevate nell’applicazione del decreto in commento;
- le ulteriori informazioni rispetto a quelle di cui al primo periodo che dovessero essere ritenute utili, relative alle attività di cui al presente decreto, previe intese tra gli Organismi di informazione per la sicurezza e l’Agenzia per la cybersicurezza nazionale.

Si osserva che tra le informazioni cui gli Organismi di informazione per la sicurezza hanno accesso sono ricomprese “le ulteriori informazioni rispetto a quelle di cui al primo periodo”. Si segnala, tuttavia, che il comma 5 consta di un solo periodo.

CAPO III – COOPERAZIONE A LIVELLO DELL'UNIONE EUROPEA E INTERNAZIONALE

Articolo 18
(Gruppo di cooperazione NIS)

L'**articolo 18** disciplina l'attività del Gruppo di cooperazione NIS, già operante ai sensi dell'abrogando **decreto legislativo n. 65 del 2018**, prevedendo che l'Autorità nazionale competente NIS partecipi alle attività del Gruppo avvalendosi, se lo richiede, del supporto delle Autorità di settore NIS sulla base delle loro specifiche competenze.

La direttiva (UE) 2022/2555 ha istituito all'**articolo 14** il Gruppo di cooperazione[7], costituito dai rappresentanti degli Stati Membri, della Commissione europea e dell'Agenzia dell'UE per la sicurezza delle reti e dell'informazione (ENISA), con il compito di implementare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri rafforzandone la fiducia reciproca.

Lo schema di decreto legislativo di recepimento prevede, in tal senso, al **comma 1** dell'articolo in commento, che sia l'Autorità nazionale competente NIS, ovvero l'Agenzia per la cybersicurezza, a partecipare al Gruppo di cooperazione NIS.

A norma dell'**articolo 8** della sopracitata direttiva, le autorità competenti NIS-*Network and Information Security* sono i soggetti cui spetta il **controllo dell'applicazione** della disposizione europea in quanto responsabili della cybersicurezza e dei compiti di vigilanza. Sono designate da ogni Stato membro il quale può affidare questo ruolo a una o più autorità esistenti. Se uno Stato membro designa o istituisce soltanto un'autorità competente, quest'ultima è anche il **punto di contatto unico** per tale Stato membro. Lo schema di decreto in commento riconosce, infatti, all'**articolo 10**, l'Agenzia per la cybersicurezza nazionale sia quale "autorità competente", che "punto di contatto unico", nonché quale "*Team* di risposta agli incidenti di sicurezza informatica (CSIRT)"[8].

---

[7] Tale Gruppo era stato già istituito con la precedente direttiva NIS, (UE) 2016/1148 che viene però abrogata dalla (UE) 2022/2555 che pone misure volte al superamento delle carenze riscontrate nella prima.

[8] L'abrogando decreto legislativo del 18 maggio 2018, n. 65 (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), c.d. NIS, dispone, invece, all'**articolo 10**, la partecipazione a tale Gruppo attraverso il Punto di contatto

Si ricorda, in tal proposito, che l'Agenzia per la cybersicurezza nazionale è stata istituita dal decreto legge del 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 legge 4 agosto 2021, n. 109.

A norma del **comma 2**, inoltre, possono essere chiamate a collaborare con l'Autorità nazionale competente NIS anche le Autorità di settore NIS ovvero, ai sensi dell'**articolo 11** dello schema di decreto legislativo in commento, la Presidenza del Consiglio dei Ministri e i singoli Ministeri, per i rispettivi ambiti di competenza.

Ai fini della loro partecipazione alle attività del Gruppo, secondo il **comma 3**, l'Autorità nazionale competente NIS e, a suo supporto, le Autorità di settore NIS, provvedono a:

a) **tenere conto degli orientamenti non vincolanti del Gruppo in merito al recepimento e all'attuazione della direttiva (UE) 2022/2555**;
b) **tenere conto degli orientamenti non vincolanti del Gruppo relativamente alle politiche in materia di divulgazione coordinata delle vulnerabilità** di cui è competente il CSIRT Italia di cui all'**articolo 16**;

L'istituzione del **CSIRT Italia** presso l'Agenzia nazionale per la cybersicurezza risponde all'obbligo, di cui **all'articolo 1, paragrafo 2 lettera a)**, **della direttiva (UE) 2022/2555**, che impone a ciascuno Stato membro di creare un organismo preposto alle funzioni di gestione degli incidenti di sicurezza[9].

c) **scambiare migliori prassi e informazioni** sia per l'attuazione della direttiva – soprattutto riguardo ai rischi, alle attività di formazione e alle specifiche tecniche anche adottate da un organismo di normazione che sia riconosciuto dal regolamento (UE) 1025/2012 – sia per identificare i soggetti essenziali e quelli importanti così come individuati dall'**articolo 6** dello schema di decreto legislativo in commento;
d) **effettuare scambi di opinione** riguardo l'attuazione di atti giuridici relativi alla cybersicurezza;

che è diversamente individuato, dall'**articolo 7**, nel Dipartimento delle informazioni per la sicurezza (DIS).

[9] In precedenza il CSIRT Italiano, era istituito presso la Presidenza del Consiglio dei Ministri dal decreto legislativo 18 maggio 2018, n. 65 (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).

e) discutere, eventualmente, le **relazioni sulla revisione tra pari** prevista dall'**articolo 19** della direttiva europea e recepita dall'**articolo 21** dello schema di decreto legislativo in commento;

L'**articolo 19 della direttiva (UE) 2022/2555**, in particolare prevede che sia il Gruppo, con l'assistenza della Commissione e dell'ENISA nonché, se del caso, della rete CSIRT ed entro il 17 gennaio 2025, a stabilire la metodologia e gli aspetti organizzativi delle revisioni volte a trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca, conseguire un livello comune elevato di cybersicurezza e migliorare le capacità e le politiche di cybersicurezza degli Stati membri. Per ulteriori approfondimenti si rimanda alla scheda relativa all'articolo 21 che disciplina nel dettaglio il tema della revisione tra pari.

f) richiedere di **aprire una discussione sulle relazioni sulla revisione** di cui sopra che coinvolgano l'Autorità nazionale competente NIS e l'elaborazione di conclusioni e raccomandazioni a riguardo;
g) **discutere sui casi di assistenza reciproca** tra cui esperienze comuni transfrontaliere di vigilanza;
h) su impulso di uno o più Stati **discutere le richieste di assistenza reciproca** di cui è competente l'Autorità nazionale competente NIS ai sensi dell'**articolo 39** dello schema di decreto legislativo in esame alla cui scheda si rimanda per ulteriori dettagli;
i) richiedere la **discussione sulle istanze specifiche di assistenza reciproca** di cui sopra;
l) **scambiare opinioni su misure per mitigare i rischi su vasta scala** sulla base degli insegnamenti tratti da **EU-CyCLON** e dalla **Rete di CSIRT nazionali**;

Si tratta di due sistemi di cooperazione, in particolare, EU-CyCLON è la rete di collegamento per le crisi informatiche che dovrebbe fungere da intermediario tra il livello tecnico e politico durante gli incidenti e le crisi di cybersicurezza, è istituita dall'**articolo 16 della direttiva europea** ed è composta da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri e, in casi particolarmente gravi, anche della Commissione.

La Rete di CSIRT è invece materia dell'**articolo 15** della medesima direttiva contribuisce allo sviluppo della fiducia e a promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri.

m) partecipare se necessario ai **programmi di sviluppo** delle capacità anche prevedendo **scambi tra il personale delle Autorità nazionali** dei diversi Stati membri;
n) **discutere sulle eventuali esercitazioni** in materia di sicurezza informatica e sulle attività dell'ENISA;

o) **partecipare alle riunioni congiunte** con il Gruppo per la resilienza dei soggetti critici definito dalla direttiva (UE) 2022/2557.

Si tratta del gruppo istituito dall'**articolo 19 della direttiva** sopra citata al fine di sostenere la Commissione e agevolare la cooperazione tra gli Stati membri e lo scambio di informazioni su questioni relative alla sicurezza dei soggetti critici, ovvero sostanzialmente dei fornitori di servizi essenziali così identificati sulla base delle indicazioni dell'**articolo 6** della medesima direttiva. Il gruppo per la resilienza dei soggetti critici è composto da rappresentanti degli Stati membri e della Commissione.

Il **comma 4 dell'articolo 18** specifica che, sempre ai fini della partecipazione alle attività del Gruppo di cooperazione, l'Autorità nazionale competente NIS, con la collaborazione delle Autorità di settore NIS interessate, contribuisce:

a) alla **definizione degli orientamenti non vincolanti di cui alla lettera a) del precedente comma**;
b) alla **definizione degli orientamenti non vincolanti di cui alla lettera b) del precedente comma**;
c) alla **definizione di pareri non vincolanti e alla cooperazione con la Commissione europea sulle nuove iniziative strategiche** in materia di sicurezza informatica;
d) alla **definizione di pareri non vincolanti e alla cooperazione con la Commissione europea sui progetti di atti delegati o di esecuzione** di cui è competente quest'ultima sulla base della stessa direttiva;
e) allo **scambio di informazioni** con tutti gli Organismi, Autorità e Istituzioni coinvolte;
f) all'**elaborazione di conclusioni su eventuali relazioni di revisione** di cui sopra;
g) all'**elaborazione delle valutazioni coordinate dei rischi** riferiti alle catene di approvvigionamento critiche relative ai servizi TIC che vengono effettuate dal Gruppo in collaborazione con la Commissione e l'ENISA come disciplina l'**articolo 22, paragrafo 1, della direttiva europea**;
h) alla **definizione degli orientamenti strategici** delle due reti di cui sopra ovvero EU-CyCLON e la Rete CSIRT nazionali su specifiche questioni emergenti;
i) al **rafforzamento delle capacità** di sicurezza informatica a livello europeo;
l) all'**organizzazione di riunioni congiunte e periodiche con i portatori di interessi** competenti del settore privato dell'unione

europea per discutere le attività dal Gruppo di cooperazione NIS traendone contributi;

m) alla **definizione della metodologia per la revisione tra pari** già menzionata **e di quella relativa all'autovalutazione** per gli Stati e all'**elaborazione di codici di condotta** per gli esperti di cybersicurezza che sono selezionati, ai sensi dell'**articolo 21, comma 2, lettera b),** dall'Autorità nazionale competente NIS, sentito Tavolo per l'attuazione della disciplina NIS, con una o più deliberazioni come stabilisce l'**articolo 40, comma 5,** dello schema di decreto in esame;

Il Tavolo di lavoro è istituito dall'**articolo 12** dello schema di decreto in esame al fine di assicurare l'implementazione e attuazione del medesimo decreto. È presieduto dal direttore generale dell'Agenzia per la cybersicurezza nazionale, o da un suo delegato, ed è composto da un rappresentante di ogni Autorità di settore NIS di cui all'**articolo 11** e da due rappresentanti designati da regioni e province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano.

n) all'**elaborazione di relazioni ai fini del riesame di cui all'articolo 40 della direttiva europea**, ovvero quelle prodotte dal Gruppo di cooperazione e di cui tiene conto la Commissione per redigere la propria, eventualmente correlata da una proposta legislativa, da presentare al Parlamento europeo e al Consiglio il 17 ottobre 2027, e successivamente **ogni 36 mesi**, sul funzionamento della direttiva stessa. La Commissione si avvale anche delle della rete di CSIRT.

o) alla **discussione e allo svolgimento di periodiche valutazioni sullo stato dei rischi**, ivi compresi i *ransomware* ovvero programmi informatici malevoli che possono inserirsi in un dispositivo digitale bloccandone l'accesso a tutti o ad alcuni dei suoi contenuti e chiedendo un riscatto per poter tornare a disporne;

p) alla **collaborazione con l'ENISA e con la Commissione europea per la pubblicazione della relazione biennale sullo stato della sicurezza informatica** dell'Unione che viene poi presentata al Parlamento europeo a norma dell'**articolo 18 della direttiva (UE) 2022/2555**;

Tale disposizione precisa che la relazione valuta, in particolare, il rischio della cybersicurezza e lo sviluppo delle capacità di cybersicurezza nei settori pubblici e privati dell'Unione, il livello generale di consapevolezza in materia tra i cittadini e i soggetti tra cui le piccole e medie imprese, il risultato delle revisioni tra pari e, infine, del livello di capacità e delle risorse di cybersicurezza anche a livello settoriale nonché del livello di allineamento delle diverse strategie nazionali. Inoltre

la relazione contiene specifiche raccomandazioni strategiche al fine di porre rimedio ad eventuali carenze.

q) Alla **collaborazione con l'ENISA, con la Commissione e con la Rete CSIRT nazionali per una definizione della metodologia** relativa alla valutazione sul livello di capacità, risorse e strategie di cybersicurezza e sull'allineamento delle strategie nazionali, come disciplinato dall'**articolo 18, paragrafo 3**, **della direttiva europea** allo scopo di redigere la relazione biennale di cui sopra.

In particolare, tale disposizione europea reca che L'ENISA, in collaborazione con la Commissione, il Gruppo di cooperazione e la rete di CSIRT, elabora la metodologia, ivi comprese le variabili pertinenti della valutazione aggregata.

Articolo 19
(Rete delle organizzazioni di collegamento per le crisi informatiche – EU-CyCLONe)

L'**articolo 19** disciplina la partecipazione dell'Agenzia per la cybersicurezza nazionale quale autorità nazionale di gestione delle crisi informatiche alla Rete delle organizzazioni di collegamento per le crisi informatiche EU-CyCLONe.

Come rilevato in premessa e nella scheda relativa agli articoli 1 e 2, la nuova disciplina recata dalla direttiva NIS2 prevede l'istituzione di una **rete europea delle organizzazioni di collegamento per le crisi informatiche EU-CyCLONe**, volta a sostenere la gestione coordinata degli incidenti di cybersicurezza su vasta scala. In questo ambito, in base al comma 1 del presente articolo, l'Agenzia - quale autorità nazionale di gestione delle crisi informatiche - contribuisce a:

- aumentare il livello di preparazione per la gestione di incidenti e crisi informatiche su vasta scala;
- sviluppare una conoscenza condivisa sui medesimi eventi;
- valutare le conseguenze dei medesimi eventi e proporre misure di attenuazione;
- coordinare la gestione dei medesimi eventi e sostenere il processo decisionale politico in materia;
- discutere, su richiesta di uno Stato membro, i piani nazionali di risposta agli incidenti e alle crisi informatiche su vasta scala previsti dall'articolo 9, paragrafo 4, della direttiva oggetto di recepimento (in base a tale norma della direttiva il piano deve, tra le altre cose, comprendere, le attività nazionali di preparazione, i compiti e le responsabilità delle autorità di gestione delle crisi informatiche e la gestione delle crisi informatiche); in relazione a tale previsione il comma 3 specifica poi che anche l'Agenzia può richiedere di discutere il piano nazionale;
- supportare la collaborazione con il gruppo di cooperazione NIS;
- cooperare con la rete di CSIRT nazionali;
- predisporre la relazione al Parlamento europeo e al Consiglio sui lavori della Rete, relazione prevista dall'articolo 16, paragrafo 7, della direttiva oggetto di recepimento (tale disposizione della direttiva prevede che la prima relazione sia preparata entro il 17 luglio 2024 e successivamente ogni 18 mesi).

Articolo 20
(Rete di CSIRT nazionali)

L'**articolo 20** regola la partecipazione del CSIRT Italia alla rete di CSIRT nazionali.

Ai sensi del **comma 1**, il CSIRT Italia partecipa alla rete di CSIRT nazionali.

Secondo quanto stabilito dal decreto legislativo n. 65 del 2018 (attuativo della direttiva UE 2016/1148, c.d. NIS) e dal DPCM 8 agosto 2019, tra i compiti del ***Computer Security Incident Response Team*** (CSIRT) italiano rientra anche la partecipazione alla rete dei CSIRT.

A tale fine, al **comma 2** si dispone che il CSIRT Italia contribuisce a:

a) scambiare informazioni per quanto riguarda le capacità dei CSIRT;
b) agevolare, ove possibile, la condivisione, il trasferimento e lo scambio di tecnologia e delle misure, delle politiche, degli strumenti, dei processi, delle migliori pratiche e dei quadri pertinenti fra i CSIRT nazionali;
c) scambiare, su richiesta di un CSIRT nazionale di un altro Stato membro potenzialmente interessato da un incidente, informazioni relative a tale incidente, alle minacce informatiche, ai rischi e alle vulnerabilità associate;
d) scambiare informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di sicurezza informatica;
e) garantire l'interoperabilità per quanto riguarda le specifiche e i protocolli per lo scambio di informazioni;
f) su richiesta di un membro della Rete di CSIRT nazionali potenzialmente interessato da un incidente, scambiare e discutere informazioni non sensibili sul piano commerciale connesse a tale incidente, ai rischi e alle vulnerabilità associati, ad eccezione dei casi in cui lo scambio di informazioni potrebbe compromettere l'indagine sull'incidente;
g) su richiesta di un membro della Rete di CSIRT nazionali, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro;
h) fornire assistenza ai CSIRT nazionali di altri Stati membri nel far fronte a incidenti che interessano due o più Stati membri;
i) cooperare e scambiare migliori pratiche con i CSIRT nazionali designati dagli altri Stati membri in qualità di coordinatori ai sensi dell'articolo 12 della direttiva (UE) 2022/2555, nonché fornire loro assistenza per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che

potrebbero avere un impatto significativo su soggetti in più di uno Stato membro;

l) discutere e individuare ulteriori forme di cooperazione operativa, anche in relazione a:
   1) categorie di minacce informatiche e incidenti; preallarmi;
   2) assistenza reciproca;
   3) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri;
   4) contributi al piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 13, comma 3, su richiesta di uno Stato membro;

m) su richiesta di un membro della Rete di CSIRT nazionali, discutere le capacità e lo stato di preparazione del CSIRT nazionale richiedente;

n) cooperare e scambiare informazioni con i centri operativi di sicurezza informatica regionali e a livello dell'Unione europea, al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche a livello dell'Unione europea;

o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 21;

p) scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi-incidenti, le minacce informatiche, i rischi e le vulnerabilità;

q) informare il Gruppo di cooperazione NIS sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera i) e, se necessario, chiedere orientamenti non vincolanti in merito;

r) fare il punto sui risultati delle esercitazioni di sicurezza informatica, comprese quelle organizzate dall'ENISA;

s) fornire orientamenti non vincolanti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.

Articolo 21
(Procedura di revisione tra pari)

L'**articolo 21** disciplina una procedura di revisione delle modalità attuative della direttiva NIS 2 - in particolare per questioni specifiche di natura transfrontaliera o intersettoriale - denominata "procedura di revisione tra pari" ai sensi dell'articolo 19 della medesima direttiva.

Ai sensi del citato articolo 19, paragrafo 1, della direttiva la procedura di revisione tra pari ha l'obiettivo di "trarre insegnamenti dalle esperienze condivise, rafforzare la fiducia reciproca, conseguire un livello comune elevato di cibersicurezza e migliorare le capacità e le politiche di cibersicurezza degli Stati membri necessarie per attuare la […] direttiva".

La direttiva prevede che entro il 17 gennaio 2025, il gruppo di cooperazione NIS (di cui all'articolo 14 della direttiva recepito all'articolo 18 del presente provvedimento) stabilisce la metodologia e gli aspetti organizzativi delle revisioni tra pari con l'assistenza della Commissione e dell'ENISA nonché, se del caso, della rete CSIRT. La partecipazione alle revisioni tra pari è volontaria ed esse sono condotte da esperti di cibersicurezza designati da almeno due Stati membri, diversi dallo Stato membro oggetto di revisione.

Il **comma 1** distingue due modalità di partecipazione alla procedura di revisione da parte dell'ACN - l'Autorità nazionale competente NIS contribuisce alla definizione della metodologia e degli aspetti organizzativi delle revisioni tra pari (nel quadro della metodologia di cui all'articolo 18, comma 4, lettera *m)*, del presente provvedimento) e può partecipare alla procedura di revisione tra pari, attraverso le seguenti due modalità distinte:

- richiedendo l'esecuzione di una revisione tra pari in relazione all'attuazione della direttiva a livello nazionale (**lett.*a*)**;
- indicando uno o più rappresentanti dell'ACN o delle Autorità di settore NIS quali esperti di sicurezza informatica per eseguire revisioni tra pari presso altri Stati membri, su richiesta di questi ultimi, nel rispetto dei codici di condotta. Eventuali rischi di conflitto di interessi riguardanti gli esperti di sicurezza informatica designati sono condivisi con gli altri Stati membri, il Gruppo di cooperazione NIS, la Commissione europea e l'ENISA prima dell'inizio della revisione tra pari (**lett. *b*)**.

Nel primo caso, ossia quando la revisione è richiesta dall'ACN – Autorità nazionale NIS, questa, con propria determinazione (**comma 2**):

- individua almeno uno dei seguenti aspetti da sottoporre alla revisione tra pari:
  - il livello di attuazione degli obblighi in materia di misure di gestione del rischio (art. 24) e di notifica degli incidenti informatici (art. 25);
  - il livello delle capacità e l'efficacia dello svolgimento dei compiti dell'Autorità medesima;
  - le capacità operative del CSIRT Italia;
  - lo stato di attuazione dell'assistenza reciproca tra l'ACN – Autorità nazionale NIS e le autorità competenti degli altri Paesi membri;
  - lo stato di attuazione degli accordi per la condivisione delle informazioni in materia di sicurezza informatica da parte die soggetti che rientrano nell'ambito di applicazione del presente provvedimenti;
  - eventuali altre questioni specifiche di natura transfrontaliera o intersettoriale;
- notifica, prima dell'inizio della revisione tra pari, agli Stati membri partecipanti, l'ambito di applicazione della medesima, comprese le questioni specifiche individuate;
- effettua un'autovalutazione degli aspetti oggetto della revisione;
- seleziona, tra gli esperti di sicurezza informatica indicati dagli altri Stati membri partecipanti, gli esperti idonei da designare. Qualora l'ACN - Autorità nazionale competente NIS si opponga alla designazione di uno o più esperti indicati, comunica allo Stato membro indicante i motivi debitamente giustificati;
- fornisce l'autovalutazione di cui sopra agli esperti designati;
- fornisce agli esperti designati le informazioni necessarie per la valutazione;
- formula osservazioni sulla relazione elaborata dagli esperti designati;
  può pubblicare la relazione elaborata dagli esperti designati.

Nel secondo caso, ossia quando la revisione è promossa da latri Stati membri, il **comma 3** individua alcuni compiti e obblighi in capo agli **esperti di sicurezza informatica** partecipanti alla revisione indicati dall'Autorità nazionale competente NIS, questi:

- non devono divulgare a terzi le eventuali informazioni sensibili o riservate ottenute nel corso delle revisioni;
- partecipano alle attività necessarie allo svolgimento delle revisioni tra pari tramite visite in loco fisiche o virtuali e scambi di informazioni a distanza;

- contribuiscono all’elaborazione delle relazioni sui risultati e sulle conclusioni delle revisioni tra pari.

Infine, ai sensi del **comma 4**, la **condivisione delle informazioni** è effettuata nel rispetto della legislazione nazionale e dell'Unione europea in materia di tutela delle informazioni protette da **classifica di segretezza** e di salvaguardia delle funzioni essenziali dello Stato, compresa la sicurezza nazionale.

L’articolo 42 della legge n. 124 del 2007 sul sistema di informazione per la sicurezza della Repubblica disciplina le classifiche di segretezza che, ai sensi di quanto disposto dal comma 1, “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”. Il comma 3 individua le classifiche attribuibili, ordinandole secondo i quattro livelli di “segretissimo, segreto, riservatissimo e riservato”. Il comma 5 prevede il meccanismo della declassificazione automatica, stabilendo che la classifica di segretezza è automaticamente declassificata a livello inferiore quando sono trascorsi cinque anni dalla data di apposizione; decorso un ulteriore periodo di cinque anni, cessa comunque ogni vincolo di classifica. Nel caso di apposizione della classifica di segretezza di riservato, decorsi cinque anni dalla data di apposizione, cessa ogni vincolo di classifica (D.L. 75/2023, art. 1, comma 4).

Articolo 22
(Comunicazioni all'Unione europea)

L'**articolo 22** individua gli obblighi di comunicazione nei confronti dell'Unione europea da parte rispettivamente della Presidenza del Consiglio dei ministri, dell'Agenzia per la cybersicurezza nazionale in qualità di Autorità nazionale competente e Punto di contatto unico NIS, nonché di Autorità nazionale di gestione delle crisi cibernetiche.

In primo luogo, dopo l'entrata in vigore del decreto in esame, la **Presidenza del Consiglio dei ministri** deve notificare tempestivamente alla Commissione europea tutte le designazioni delle **autorità competenti** (**comma 1**). Pertanto:

- la conferma dell'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS e quale Punto di contatto unico NIS,
- la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e del Ministero della difesa, quali Autorità nazionali di gestione delle crisi informatiche, e i relativi ambiti di competenza come indicati all'articolo 2, comma 1, lettera g).

Ogni successiva ulteriore modifica a tali designazioni o compiti deve essere ulteriormente notificata, senza ingiustificato ritardo. Alle designazioni sono assicurate idonee forme di pubblicità.

Ai sensi del **comma 2**, l'Agenzia per la cybersicurezza nazionale, in qualità di **autorità nazionale competente** trasmette alla Commissione europea la Strategia nazionale di cybersicurezza e i suoi aggiornamenti. Inoltre ha una serie di obblighi di comunicazione alla Commissione relativi al numero dei e ad informazioni sui soggetti essenziali e su quelli importanti individuati a livello nazionale (ivi incluse le misure sanzionatorie e le disposizioni sulle sanzioni).

Infine alcune informazioni sui soggetti e sui soggetti importanti devono essere comunicate all'ENISA, ai fini del loro inserimento nel registro di cui all'articolo 27 della direttiva (UE) 2022/2555. L'Autorità nazionale competente NIS può richiedere ad ENISA l'accesso a tale registro, assicurando la tutela della riservatezza delle informazioni ivi contenute.

L'Agenzia per la cybersicurezza nazionale, in qualità di **Punto di contatto unico NIS** (**comma 3**) comunica in primo luogo alla Commissione europea

le designazioni relative al CIRST Italia, anche quale coordinatore in materia di divulgazione delle vulnerabilità, con i relativi compiti. Inoltre trasmette all'ENISA:

- una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti, con cadenza trimestrale a partire dal 1° gennaio 2026;
- senza ingiustificato ritardo, le notifiche di incidente con effetti transfrontalieri di cui agli articoli 25 e 26 (la trasmissione è prevista anche ai punti di contatto unici degli altri Stati membri interessati)

Infine, ai sensi del **comma 4**, in qualità di **Autorità nazionale di gestione delle crisi informatiche**, l'Agenzia comunica alla Commissione europea e alla Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) entro tre mesi dall'adozione o dall'aggiornamento del Piano nazionale di risposta agli incidenti e alle crisi informatiche su larga scala (su cui si v., *supra*, articolo 13), le informazioni del Piano, fatto salvo quanto previsto dall'articolo 4, commi 1, 6 e 7, che stabilisce alcuni limiti al campo di applicazione dello schema di decreto in esame.

Le disposizioni richiamate in particolare stabiliscono che gli obblighi stabiliti nel decreto in attuazione della direttiva NIS2 non possono **mai** comportare la **divulgazione d'informazioni sensibili per gli interessi essenziali** dello Stato.

CAPO IV – OBBLIGHI IN MATERIA DI GESTIONE DEL RISCHIO PER LA SICUREZZA INFORMATICA E DI NOTIFICA DI INCIDENTE

Articolo 23
(Organi di amministrazione e direttivi)

L'**articolo 23** disciplina gli obblighi e le responsabilità degli organi di amministrazione e direttivi dei soggetti essenziali e importanti.

L'articolo 23 consta di tre commi e recepisce alcune disposizioni contenute all'articolo 20, in materia di ***governance***, della direttiva 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022.

Il **comma 1** impone alcuni adempimenti in materia di sicurezza informatica a carico degli organi di amministrazione e degli organi direttivi dei soggetti essenziali e dei soggetti importanti.

Nel rinviare alla scheda dell'articolo 6 per approfondimenti, si ricorda che sono "**soggetti essenziali**":

- i soggetti operanti nei settori ad alta criticità indicati nell'allegato I che superano i massimali per le medie imprese (occupanti più di 249 persone e il cui fatturato annuo superi i 50 milioni di euro oppure il cui totale di bilancio annuo superi i 43 milioni di euro);
- i soggetti identificati come "soggetti critici" ai sensi del decreto legislativo, attualmente all'esame delle Camere (A.G. 165), che recepisce la direttiva (UE) 2022/2557, indipendentemente dalle loro dimensioni;
- i fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico aventi i requisiti dimensionali delle medie imprese;
- i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, indipendentemente dalle loro dimensioni;
- pubbliche amministrazioni centrali, indipendentemente dalle loro dimensioni (Organi costituzionali e di rilievo costituzionale ma con esclusione del Parlamento, Presidenza del Consiglio dei ministri e Ministeri, Agenzie fiscali e Autorità amministrative indipendenti);
- i soggetti, indipendentemente dalle loro dimensioni, individuati dall'Autorità nazionale competente NIS (e cioè l'Agenzia per la cybersicurezza nazionale) nell'ambito: delle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III; dei soggetti delle

tipologie di cui all'allegato IV (soggetti che forniscono servizi di trasporto pubblico locale, istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, società *in house*, società partecipate e società a controllo pubblico, come definite nel D.Lgs. n. 175/2016); dei soggetti delle tipologie di cui agli allegati I (settori ad alta criticità), II (settori critici) e IV (ulteriori tipologie di soggetti), indipendentemente dalle loro dimensioni, laddove soddisfino determinati requisiti; delle imprese collegate ad un soggetto essenziale o importante, se soddisfa determinati requisiti (art. 3, co. 10).

Sono "**soggetti importanti**" tutti i soggetti pubblici e privati che rientrano nell'ambito di applicazione del decreto (articolo 3) e che non sono considerati essenziali.

La lettera **a) del comma 1** impone agli organi di amministrazione e agli organi direttivi dei soggetti essenziali e dei soggetti importanti di approvare le modalità di messa a punto delle misure di gestione dei rischi per la sicurezza informatica adottate, dagli stessi soggetti essenziali e importanti, ai sensi dell'articolo 24.

Si ricorda che l'articolo 24 impone ai soggetti importanti e ai soggetti essenziali di adottare misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi nell'ambito della sicurezza dei sistemi informativi. Le misure, basate su un **approccio multi-rischio** devono comprendere una serie di elementi elencati nella disposizione. Si stabilisce, poi, con specifico riferimento alla valutazione dell'adeguatezza della sicurezza nella catena di approvvigionamento, che vengano considerate le vulnerabilità specifiche di ciascun fornitore, la qualità dei loro prodotti e delle pratiche di sicurezza informatica, comprese le procedure di sviluppo sicuro. Inoltre, deve essere tenuto conto dei risultati delle valutazioni dei rischi effettuate, nell'ambito della sicurezza delle catene di approvigionamento, dal Gruppo di cooperazione NIS.

La lettera **b) del comma 1** impone agli organi di amministrazione e agli organi direttivi dei soggetti essenziali e dei soggetti importanti di sovrintendere all'attivazione degli obblighi del capo IV e di cui all'articolo 7 del decreto.

Il capo IV del decreto in commento è dedicato obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente. In particolare, si ricordano gli **obblighi in materia di misure di gestione dei rischi per la sicurezza informatica** (articolo 24), gli **obblighi in materia di notifica di incidente** (articolo 25), nonché la disciplina relativa alla **proporzionalità e gradualità degli obblighi** (articolo 31).

La lettera **c) del comma 1** dispone che gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti siano

responsabili delle violazioni del decreto in commento compiute dagli stessi soggetti.

Il **comma 2** pone alcuni obblighi con riferimento alla formazione in materia di sicurezza informatica.

Si ricorda che la formazione è oggetto di promozione e sviluppo nell'ambito della **strategia nazionale per la cybersicurezza** e costituisce, appunto, una misura strategica in tale materia (articolo 9, comma 3, lettera f). Le attività di formazione costituiscono, inoltre, una misura nazionale di preparazione con riferimento al **piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala** (articolo 13, comma 4, lettera d). È opportuno, poi, ricordare che le pratiche di formazione sono ricomprese tra gli elementi utili ai fini dell'adozione delle **misure di gestione dei rischi per la sicurezza informatica** da parte dei soggetti essenziali e dei soggetti importanti (articolo 24, comma 2, lettera g).

In particolare, la **lettera a) del comma 2** impone agli organi di amministrazione e agli organi direttivi dei soggetti essenziali e dei soggetti importanti di seguire una formazione in materia di sicurezza informatica.

Secondo quanto disposto, poi, alla **lettera b) del comma 2**, gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti promuovono l'offerta periodica di una formazione, coerente con quella in materia di sicurezza informatica seguita dagli organi citati, in favore dei loro **dipendenti**. Tale formazione è finalizzata a favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica, nonché il loro impatto sulle attività del soggetto (essenziale o importante) e sui servizi offerti.

Il **comma 3** prevede che gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti siano informati periodicamente o, se opportuno, tempestivamente, degli incidenti e delle notifiche di cui agli articoli 25 e 26.

L'articolo 25 pone una serie di obblighi in materia di **notifica di incidente**. In particolare, al comma 1 è previsto che i soggetti essenziali e i soggetti importanti debbano notificare al CSIRT Italia (Gruppo nazionale di risposta agli incidenti di sicurezza operante all'interno dell'Agenzia per la cybersicurezza nazionale) ogni incidente che abbia un impatto significativo sulla fornitura dei loro servizi.

L'articolo 26 disciplina, invece, la **notifica volontaria di informazioni pertinenti**.

Articolo 24
(Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica)

L'**articolo 24,** composto da **4 commi**, prevede una serie di obblighi per i **soggetti essenziali** e i **soggetti importanti** al fine di gestire i rischi per la sicurezza informatica. In particolare, prevede l'obbligo di adottare misure **tecniche, operative e organizzative** adeguate e proporzionate alla gestione dei rischi, specificandone le caratteristiche e gli elementi essenziali.
Infine, stabilisce che, per **valutare l'adeguatezza delle misure di sicurezza nella catena di approvvigionamento**, i citati soggetti considerino le vulnerabilità specifiche di ogni fornitore e la qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei fornitori, incluse le loro procedure di sviluppo sicuro. Devono anche tenere conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal **Gruppo di cooperazione NIS**.

Il **comma 1** introduce l'obbligo per i **soggetti essenziali** e i **soggetti importanti** di adottare **misure tecniche, operative e organizzative** adeguate e proporzionate alla **gestione dei rischi** per la sicurezza informatica, secondo le modalità e i termini di cui agli articoli 30, 31 e 32 (v. *infra*). In particolare, dispone che tali misure:

- assicurano un **livello di sicurezza** dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;
- sono **proporzionate** al grado di **esposizione** a rischi del soggetto, alle **dimensioni** del soggetto e alla **probabilità** che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.

Il **comma 2** specifica che tali misure siano basate su un approccio **multi-rischio**, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendano anche i seguenti elementi:

a) politiche di **analisi dei rischi e di sicurezza** dei sistemi informativi e di rete;
b) **gestione degli incidenti,** ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26 (v. *infra*);
c) **continuità operativa,** ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;

d) **sicurezza della catena di approvvigionamento**, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
e) **sicurezza dell'acquisizione**, dello **sviluppo** e della **manutenzione** dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;
f) politiche e procedure per valutare l'**efficacia delle misure** di gestione dei rischi per la sicurezza informatica;
g) pratiche di **igiene** di base e di formazione in materia di sicurezza informatica;
h) politiche e procedure relative all'uso della **crittografia** e, ove opportuno, della **cifratura**;
i) **sicurezza e affidabilità del personale,** politiche di controllo dell'accesso e gestione dei beni e degli assetti;
j) uso di soluzioni di **autenticazione a più fattori** o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.

Il **comma 3**, al fine di valutare l'adeguatezza delle misure **sicurezza della catena di approvvigionamento** (di cui alla lettera *d)* del comma 2 dell'articolo in esame), indica che i soggetti devono tenere conto delle **vulnerabilità specifiche** per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro.

Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

Infine, il **comma 4** specifica che qualora un soggetto rilevi di non essere conforme alle misure di cui al comma 2, esso adotta, senza indebito ritardo, tutte le misure appropriate e proporzionate correttive necessarie.

Articolo 25, commi 1-6
(Obblighi in materia di notifica di incidente)

L'**articolo 25** si compone di **12 commi** volti ad introdurre una serie di obblighi in materia di **notifica degli incident**i. In particolare, come prescritto anche dalla direttiva NIS2, nei primi sei commi sono previste le seguenti tempistiche: una **pre-notifica**, **entro 24 ore** da quando i soggetti sono venuti a conoscenza dell'incidente significativo; successivamente, una **notifica entro 72 ore;** una eventuale **relazione intermedia**, su richiesta del CSIRT Italia; infine, una **relazione finale**, entro **un mese** dalla trasmissione della notifica.

L'**articolo 25, commi 1-3,** impone l'obbligo per i **soggetti essenziali e i soggetti importanti** di **notificare,** senza ingiustificato ritardo, al CSIRT Italia ogni **incidente** che ha un **impatto significativo sulla fornitura dei loro servizi,** secondo le modalità e i termini di cui agli articoli 30, 31 e 32 (v. *infra*). Tale notifica deve includere le informazioni che consentano al CSIRT Italia di determinare un **eventuale impatto transfrontaliero** dell'incidente. In generale, la notifica non espone il soggetto effettuante ad una maggiore responsabilità rispetto a quella derivante dall'incidente.

Il **comma 4** specifica che un **incidente è considerato significativo** se:

- ha causato o è in grado di causare una **grave perturbazione operativa** dei servizi o **perdite finanziarie** per il soggetto interessato;
- ha avuto **ripercussioni** o è idoneo a provocare ripercussioni su **altre persone fisiche o giuridiche** causando perdite materiali o immateriali considerevoli.

Il **comma 5** dell'articolo in commento, detta le tempistiche relative alla suddetta notifica. In particolare, i soggetti trasmettono al CSIRT Italia senza ingiustificato ritardo:

a) **entro 24 ore** da quando sono venuti a conoscenza dell'incidente significativo, una **pre-notifica** che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di **atti illegittimi o malevoli** o può avere un **impatto transfrontaliero**;
b) **entro 72 ore** da quando sono venuti a conoscenza dell'incidente significativo, una **notifica dell'incidente** che, ove possibile, aggiorni le informazioni di cui alla lettera a) e indichi una **valutazione iniziale**

dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

- In **deroga** a questa disposizione, il **comma 6** prevede che i **prestatori di servizi fiduciari** comunico gli incidenti significativi impattanti sui propri servizi fiduciari entro **24 ore** da quando ne sono venuti a conoscenza;

c) su richiesta del CSIRT Italia, **una relazione intermedia** sui pertinenti aggiornamenti della situazione;

d) una **relazione finale** entro **un mese** dalla **trasmissione** della notifica dell'incidente di cui alla lettera b), che comprenda:

- una **descrizione dettagliata** dell'incidente, ivi inclusi la sua gravità e il suo impatto;
- il **tipo di minaccia** o la **causa originale** (*root cause*) che ha probabilmente innescato l'incidente;
- le misure di **attenuazione** adottate e in corso;
- ove noto, l'**impatto transfrontaliero** dell'incidente.

e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), una **relazione mensile** sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

Articolo 25, commi 7-8
(Obblighi in materia di notifica di incidente)

L'**articolo 25,** ai **commi 7 e 8,** disciplina gli obblighi relativi alla risposta del CSIRT Italia al soggetto notificante.

Il **comma 7** prevede che il **CSIRT Italia fornisca una risposta al soggetto notificante,** comprensiva di un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza sull'attuazione di possibili misure tecniche di mitigazione. Su richiesta del soggetto notificante, il CSIRT Italia fornisce ulteriore **supporto tecnico**.

Il **comma 8** specifica che in caso di sospetto relativo al **carattere criminale dell'incidente,** il CSIRT Italia **notifichi anche l'Autorità di Contrasto,** istituita presso l'organo centrale del Ministero dell'Interno per la regolarità dei servizi di telecomunicazione.

L'articolo 7-*bis* del decreto-legge n. 144 del 2005 recante misure urgenti per il contrasto al **terrorismo internazionale**, convertito, con modificazioni, dalla legge n. 155 del 2005, dispone che l'**organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione** assicura i servizi di **protezione informatica** delle **infrastrutture critiche informatizzate** di **interesse nazionale** individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

Articolo 25, commi 9-10
(Obblighi in materia di notifica di incidente)

L'**articolo 25,** ai **commi 9 e 10,** disciplina gli obblighi relativi alle eventuali comunicazioni sa parte dei soggetti importanti e essenziali ai destinatari dei loro servizi a seguito di un incidente o una minaccia informativa significativa.

I **commi 9 e 10**, prevedono, rispettivamente, che i **soggetti essenziali e i soggetti importanti** comunichino tempestivamente ai destinatari dei loro servizi, sentito il CSIRT Italia e se ritenuto opportuno e qualora possibile:

- gli incidenti significativi che possono ripercuotersi negativamente sulla **fornitura** di tali servizi;
- che sono **potenzialmente interessati** da una minaccia informatica significativa, specificandone anche **la natura**, indicando altresì **misure o azioni correttive** o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia.

Articolo 25, commi 11-12
(Obblighi in materia di notifica di incidente)

L'**articolo 25,** ai **commi 11** e **12,** reca disposizioni relative alle **attività dell'ACN** in merito alle **comunicazioni** inerenti agli **incidenti significativi.**

Il **comma 11** dell'articolo in esame dispone che l'ACN – in qualità di autorità nazionale competente NIS e CSIRT Italia – possa, sentendo anche le autorità competenti e gli CSIRT nazionali di altri stati membri interessati, **informare il pubblico** in merito all'**incidente significativo** al fine di evitarne altri o per gestirlo, o qualora ritenga che tale divulgazione sia nell'**interesse pubblico.**

Il **comma 12** dispone che l'ACN adotta mezzi tecnici e relative procedure per semplificare le notifiche di cui al presente articolo e le notifiche volontarie di cui all'articolo 26 (v. *infra*), informando i soggetti essenziali e i soggetti importanti.

Articolo 26
(Notifica volontaria di informazioni pertinenti)

L'**articolo 26** disciplina la possibilità per alcuni soggetti di trasmettere al CSIRT, su base volontaria, informazioni su incidenti, minacce o quasi-incidenti relativi alla fornitura dei loro servizi. La disposizione si aggiunge a quanto disposto dall'**articolo 25** dedicato ai casi per i quali ricade l'obbligo di notifica.

La disposizione in commento, riprendendo quanto disposto dall'**articolo 30** della direttiva (UE) 2022/2555, prevede in aggiunta alla notifica di incidente, di natura obbligatoria, prevista dall'**articolo 25** alcuni casi di trasmissione di segnalazioni al **CSIRT Italia** su base volontaria.

Si ritiene opportuno ricordare anche in questa sede che il **CSIRT – *Computer Emergency Response Team*** – è definito dalla direttiva (UE) 2016/1148 quale "gruppo di intervento per la sicurezza informatica in caso di incidente" che ogni Stato membro è chiamato a istituire con il compito di trattare gli incidenti e i rischi secondo una procedura definita. Il CSIRT Italia è istituito presso la Presidenza del Consiglio dall'**articolo 8** del decreto legislativo 18 maggio 2018, n. 65 (Attuazione della cd. "direttiva NIS") fino alla modifica intercorsa con il decreto legge n. 82 del 2021 che lo ha trasferito presso l'Agenzia per la cybersicurezza nazionale mutuandone il nome che precedentemente era CSIRT italiano. La **direttiva (UE) 2022/2555**, che abroga quella di cui sopra, ne replica la disciplina all'**articolo 1, paragrafo 2, lettera a)**. Di conseguenza, e conformemente a tale disposizione, l'**articolo 11** dello schema di decreto in commento ne aggiorna la disciplina.

Il **comma 1, lettera a),** dispone che i soggetti essenziali e i soggetti importanti, così come definiti dall'**articolo 6**, possono notificare incidenti diversi da quelli indicati dal **comma 1 dell'articolo 25** – ovvero quelli capaci di provocare un impatto significativo sulla fornitura dei loro servizi – minacce o quasi-incidenti.

Gli **incidenti con impatto significativo sulla fornitura dei servizi** sono individuati dal **comma 4 dell'articolo 25** come quelli relativi ad una grave disfunzione o a perdite finanziarie oppure che comportano o possono comportare ripercussioni su altre persone fisiche o giuridiche o causare perdite materiali o immateriali per il soggetto interessato.

Le **minacce**, come richiamato dall'**articolo 6, comma 1,** sono definite all'**articolo 2** del regolamento (UE) 2019/881 come "qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone".

I **quasi-incidenti** trovano, invece, la loro definizione all'**articolo 6, paragrafo 1**, **della direttiva** e sono tutti quegli eventi che avrebbero potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi informatici e di rete o accessibili attraverso di essi, ma che sono stati efficacemente evitati o non si sono verificati.

La **lettera b) del comma 1**, statuisce che anche altri soggetti diversi da quelli individuati dalla **lettera a)** e indipendentemente dal fatto che ricadano nell'ambito di applicazione dello schema di decreto in commento possono trasmettere le informazioni sugli incidenti che hanno un impatto significativo sulla fornitura dei loro servizi o in caso di minacce o quasi-incidenti.

Il **comma 2** reca disposizioni sulle funzioni del CSIRT Italia in caso di trasmissione di notifica volontaria.

In particolare, la **lettera a)** dispone si applichi la medesima procedura di cui all'**articolo 25** ovvero che il CSIRT Italia fornisca una risposta al soggetto notificante, con un primo riscontro e, se richiesti, consulenza e sostegno tecnico per le misure di intervento (**comma 7**). Inoltre, in caso si sospetti il carattere criminale dell'azione notificata il CSIRT Italia fornisce al soggetto colpito anche gli orientamenti per una segnalazione diretta all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo **7-*bis*** del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (**comma 8**).

Si tratta dell'Autorità di contrasto a cui compete assicurare i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno.

Il **comma 2**, **alla lettera b),** precisa che il CSIRT Italia deve trattare con priorità le notifiche obbligatorie disciplinate dall'**articolo 25** rispetto a quelle volontarie e, alla **lettera c),** che può occuparsi di quest'ultime solo se ciò non costituisca un onere sproporzionato o eccessivo.

Infine, il **comma 3**, dispone che la notifica volontaria non fa sorgere in capo ai soggetti notificanti alcun obbligo che non sia legato ad esigenze di indagine, accertamento perseguimento di reati.

Articolo 27
(Schemi certificazione cybersicurezza)

L'**articolo 27** conferisce all'Agenzia per la cybersicurezza nazionale in quanto Autorità nazionale competente NIS la possibilità di imporre ai "soggetti essenziali" e ai "soggetti importanti" l'utilizzo di determinati prodotti, servizi e processi TIC (tecnologie dell'informazione e della sicurezza).

Per la definizione di "soggetti essenziali" e "soggetti importanti" si rinvia alle schede di lettura degli articoli 6 e 7.

Le definizioni di "prodotti TIC", "servizi TIC" e "processi TIC" sono invece presenti all'articolo 2, comma 1, rispettivamente alle lettere ff), gg) e hh) del provvedimento in esame. In particolare:

- è un prodotto TIC un elemento o un gruppo di elementi di un sistema informativo o di rete;
- è un servizio TIC un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo dei sistemi informativi e di rete;
- è un processo TIC un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC.

Il **comma 1** specifica che l'Agenzia potrà procedere attraverso le modalità di cui all'articolo 40, comma 5, cioè con l'adozione di determinazioni dell'Agenzia sentito il Tavolo per l'attuazione della disciplina NIS istituito dall'articolo 12 (cfr. *supra* la relativa scheda di lettura).

Il comma 1 specifica altresì che l'Agenzia potrà imporre a soggetti essenziali e soggetti importanti l'utilizzo sia di prodotti, servizi e processi TIC da loro stessi sviluppati sia di altri acquistati da terze parti.

Sempre in base al comma 1 i prodotti, servizi e processi TIC dovranno essere certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza previsti dall'articolo 49 del regolamento (UE) 2019/881. Tale articolo disciplina, a livello di Unione europea, la preparazione, adozione e revisione di un sistema europeo di certificazione della cybersicurezza. Tra le altre cose, si prevede che sia l'Agenzia europea per la cybersicurezza, l'ENISA a preparare una proposta in materia dopo aver consultato tutti i

portatori di interessi. Sulla proposta dell'ENISA è raccolto il parere dell'ECCG, cioè il gruppo europeo per le certificazioni in materia di cybersicurezza, che riunisce le autorità nazionali in materia. È la Commissione europea ad adottare infine il sistema di certificazione.

Il comma 1 prevede inoltre che l'Agenzia promuova anche l'utilizzo, da parte dei soggetti essenziali e dei soggetti importanti, di servizi fiduciari qualificati. L'articolo 2, comma 1, lettera uu) del provvedimento in esame definisce il concetto di "servizio fiduciario qualificato" attraverso il richiamo alle definizioni del regolamento (UE) n. 910 del 2014. In sostanza, per servizio fiduciario si intende un servizio elettronico fornito normalmente dietro remunerazione e consistente nella creazione, verifica e convalida delle firme elettroniche, di sigilli elettronici, di certificati di autenticazione di siti web. Il servizio fiduciario è qualificato quando risponde a tutti i requisiti del regolamento (UE) n. 910 del 2014.

Il comma 1 infine individua la finalità della disposizione nel garantire il rispetto, da parte di soggetti essenziali e di soggetti importanti, di "determinati" obblighi in materia di misure di gestione dei rischi per la sicurezza informatica previsti dall'articolo 24 (per approfondimenti si veda la relativa scheda di lettura).

Il **comma 2** specifica che l'Agenzia può procedere a quanto previsto dal comma 1 anche nelle more dell'adozione dei sistemi europei di certificazione della cybersicurezza, con la medesima procedura del comma 1. In questo caso si deve però trattare di prodotti, servizi e processi TIC che siano certificati nell'ambito di schemi di certificazione riconosciuti a livello nazionale o europeo.

Articolo 28
(Specifiche tecniche)

L'**articolo 28** attribuisce all'Autorità nazionale competente NIS (cioè l'Agenzia per la cybersicurezza nazionale) la facoltà di **promuovere l'uso di specifiche tecniche**, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, nonché di predisporre e aggiornare periodicamente un elenco delle categorie di tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di gestione dei rischi per la sicurezza informatica, tenendo conto delle linee guida e degli orientamenti non vincolanti elaborati da ENISA, l'Agenzia europea per la cybersicurezza.

Per favorire l'attuazione efficace e armonizzata delle misure di gestione dei rischi di sicurezza cibernetica, ai sensi del **comma 1** l'Autorità nazionale competente NIS promuove l'uso di specifiche tecniche europee e internazionali, anche adottate da un organismo di normazione riconosciuto di cui al regolamento (UE) 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, relative alla sicurezza dei sistemi informativi e di rete, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia.

A tal fine, al **comma 2** si dispone che l'Autorità nazionale competente NIS tenga conto delle linee guida e degli orientamenti non vincolanti elaborati da ENISA ai sensi dell'articolo 25, paragrafo 2, della direttiva (UE) 2022/2555.

La medesima Autorità può, inoltre, redigere e aggiornare periodicamente un elenco delle categorie di tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di gestione dei rischi per la sicurezza informatica.

Al **comma 3** si precisa che tale elenco – il quale non ha carattere vincolante o esaustivo – è pubblicato sul sito dell'Agenzia per la cybersicurezza nazionale al fine di fornire un orientamento sulle specifiche tecniche, di cui al comma 1, e sulle norme di settore nazionali ed europee applicabili alle tipologie di soggetti di cui agli allegati I, II, III e IV al presente decreto (per l'illustrazione del contenuto di tali allegati si rinvia alla scheda di lettura relativa all'articolo 3).

Articolo 29
(Banca dei dati di registrazione dei nomi di dominio)

L'**articolo 29** si compone di **7 commi** e prevede che **i gestori di registri e i fornitori di servizi di registrazione di domini di primo livello** raccolgono e mantengono accurati **dati di registrazione** conformemente al diritto dell'Unione europea in materia di protezione dei dati personali.
Il **comma 2** specifica che i dati raccolti debbano includere: nome di dominio, data di registrazione, contatti del registrante e amministratore (nome, email, telefono).
Il **comma 3** indica che i **gestori e fornitori** devono **pubblicare politiche e procedure** per assicurare la **completezza** e **accuratezza** dei **dati.** Il **comma 4** dispone che i **dati non personali di registrazione** devono essere resi **pubblicamente disponibili subito dopo la registrazione.**
Il **comma 5** impone l'obbligo, previa **richiesta motivata,** di fornire **i dati di registrazione specifici entro 72 ore,** sempre in conformità alla disciplina unionale in materia A tal fine, il **comma 6** indica che l'ACN può **richiedere l'accesso ai dati** e **stipulare protocolli** con i gestori e fornitori.
Infine, il **comma 7** specifica che al fine di **evitare duplicazioni**, gestori e fornitori devono **collaborare** nella **raccolta** e **mantenimento dei dati.**

Il **comma 1** dell'articolo 29 prevede che, al fine di contribuire alla sicurezza, alla stabilità e alla resilienza dei sistemi di nomi di dominio, i **gestori di registri dei nomi di dominio di primo livello** e i **fornitori di servizi di registrazione dei nomi di dominio** raccolgono e mantengono dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati con la dovuta diligenza, conformemente al diritto dell'Unione europea in materia di protezione dei dati personali.

Il **comma 2** specifica che la **banca dei dati** di registrazione dei nomi di dominio contiene le informazioni necessarie per identificare e contattare i titolari dei **nomi di dominio** e i **punti di contatto che amministrano i nomi di dominio sotto i TLD (*top level domain*)**. Tali informazioni includono, almeno:

- il nome di dominio;
- la data di registrazione;
- il nome, l'indirizzo e-mail di contatto e il numero di telefono del soggetto che procede alla registrazione;

- l'indirizzo e-mail di contatto e il numero di telefono del punto di contatto che amministra il nome di dominio qualora siano diversi da quelli del soggetto che procede alla registrazione.

I **commi 3-5** prevedono i seguenti obblighi per i gestori e fornitori:

- il **comma 3** dispone che predispongono e **rendono pubbliche politiche e procedure**, incluse le procedure di verifica, al fine di garantire che le banche dati di cui al comma 1 contengano informazioni accurate e complete;
- Il **comma 4** prevede che **rendono pubblicamente disponibili**, senza ingiustificato ritardo dopo la registrazione di un nome di dominio, i dati di registrazione dei nomi di dominio che **non sono dati personali**.
- Il **comma 5** dispone che, su **richiesta motivat**a dei soggetti legittimati, i gestori e i fornitori forniscono l'**accesso a specifici dati di registrazione dei nomi di dominio,** nel rispetto del diritto dell'Unione europea in materia di protezione dei dati. Essi devono **rispondere** senza ingiustificato ritardo e, comunque, e**ntro 72 ore** dalla ricezione della richiesta di accesso. Tale risposta deve contenere gli **specifici dati** di registrazione dei nomi di dominio richiesti, ovvero le motivazioni per cui la richiesta non è stata ritenuta legittima o debitamente motivata. Le politiche e le procedure relative alla divulgazione di tali dati hanno **evidenza pubblica.**

Ai fini del comma 5, il **comma 6** prevede che **l'ACN** può richiedere l'**accesso ai dati di registrazione dei nomi di dominio** e può stipulare appositi **protocolli** con i gestori di registri dei nomi di dominio di primo livello e i fornitori di registrazione dei nomi di dominio.

Al fine di evitare una duplicazione della raccolta di dati di registrazione dei nomi di dominio, il **comma 7** indica che i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio individuano **modalità e procedure di collaborazione per la raccolta e il mantenimento dei dati** di cui al comma 1.

Articolo 30
(Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi)

L'**articolo 30** dispone che i **soggetti importanti** e i **soggetti essenziali** dal 1° maggio al 30 giugno di ogni anno comunichino e aggiornino un **elenco** delle proprie **attività** e dei propri **servizi**.

In particolare, si tratta di un meccanismo di elencazione e di distinzione in categorie delle attività e dei servizi svolti dai soggetti importanti e dai soggetti essenziali, come individuati dall'articolo 6 del provvedimento in esame, alla cui scheda di lettura si rinvia. A partire dalla conferma tramite piattaforma digitale dell'iscrizione nell'elenco dei soggetti importanti ed essenziali (si veda l'art. 7), questi, procedono alla comunicazione e all'aggiornamento di un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari per definirne i caratteri ai fini della relativa classificazione. La comunicazione e l'aggiornamento vengono effettuati, ogni anno, dal 1° maggio al 30 giugno di ogni anno.

La direttiva NIS 2 oggetto di recepimento con il presente provvedimento non contempla obblighi di comunicazione come quelli previsti dall'articolo in esame. Tuttavia, come si legge nella relazione illustrativa, se ne prevede l'introduzione "al fine di consentire l'applicazione proporzionata e graduale degli obblighi della direttiva (previsti dall'articolo 32 del presente decreto), in linea con quanto previsto dal considerando 124 della direttiva stessa[10]".

La direttiva affida agli Stati membri il compito di provvedere affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività

[10] Il considerando 124 prevede quanto segue: "Nell'esercizio della vigilanza ex ante, le autorità competenti dovrebbero poter decidere in modo proporzionato l'ordine di priorità nel ricorso alle misure e ai mezzi di vigilanza a loro disposizione. Ciò implica che le autorità competenti possano decidere l'ordine di priorità sulla base di metodologie di vigilanza che dovrebbero seguire un approccio basato sui rischi. Più specificamente, tali metodologie potrebbero includere criteri o parametri di riferimento per la classificazione dei soggetti essenziali in categorie di rischio e corrispondenti misure e mezzi di vigilanza raccomandati per categoria di rischio, quali l'uso, la frequenza o il tipo di ispezioni in loco, audit sulla sicurezza mirati o scansioni di sicurezza, il tipo di informazioni da richiedere e il livello di dettaglio di tali informazioni. Tali metodologie di vigilanza potrebbero inoltre essere corredate da programmi di lavoro ed essere valutate e riesaminate periodicamente, anche per quanto riguarda aspetti quali l'assegnazione e il fabbisogno di risorse. In relazione agli enti della pubblica amministrazione, i poteri di vigilanza dovrebbero essere esercitati in linea con i quadri legislativi e istituzionali nazionali".

o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi (così articolo 21 della direttiva NIS 2 recepita dall'articolo 24 del provvedimento in esame, alla cui scheda di lettura si rinvia).

Il procedimento di elencazione prevede, in primo luogo che l'Agenzia per la cybersicurezza nazionale (ACN) in quanto Autorità nazionale competente NIS stabilisca, con propria determinazione e sentito il Tavolo per l'attuazione della disciplina NIS (istituito dall'articolo 12, per approfondimenti si rinvia alla scheda di lettura di tale articolo), anche tenuto conto degli obblighi di notifica degli incidenti da parte dei soggetti essenziali e dei soggetti importanti (ai sensi di quanto previsto dall'articolo 25, comma 1), definisca le categorie di rilevanza il processo, le modalità e i criteri per l'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi (**comma 2**).

I soggetti interessati trasmettono dal 1° maggio al 30 giugno di ogni anno un **elenco** delle proprie **attività** e dei propri **servizi (comma 1)** e nei successivi 90 giorni dalla comunicazione, l'ACN fornisce **riscontro** ai soggetti essenziali e ai soggetti importanti circa la conformità di quanto comunicato rispetto alle modalità e ai criteri di cui sopra. Il termine di cui sopra può essere prorogato per una sola volta e fino ad un massimo di ulteriori 60 giorni. Se è necessario richiedere integrazioni e informazioni aggiuntive ai soggetti essenziali o importanti, i termini di cui al presente comma sono interrotti sino alla data di ricevimento delle predette integrazioni e informazioni, che sono rese entro il termine di 30 giorni dalla richiesta (**comma 3)**. In assenza del riscontro vale il principio del silenzio-assenso e alla scadenza dei termini di cui sopra la conformità di si intende convalidata (**comma 4**).

Infine, ai sensi del **comma 5**, per l'espletamento di tali attività, l'ACN - può avvalersi dei tavoli settoriali istituiti per i rispettivi settori di competenza dalla medesima ACN di cui all'articolo 11, comma 4, lettera *f)* del provvedimento in esame.

Articolo 31
(Proporzionalità e gradualità degli obblighi)

L'**articolo 31** stabilisce che l'Agenzia, in qualità di Autorità nazionale competente NIS, adotti **criteri di proporzionalità e gradualità** nella definizione degli **obblighi** in materia di gestione del rischio di sicurezza cibernetica e di notifica di incidenti. La norma attribuisce poi alla medesima Agenzia il potere di stabilire termini, modalità, specifiche e tempi graduali di implementazione di tali obblighi.

In particolare, il **comma 1** dispone che l'Agenzia preveda **obblighi** in materia di gestione del rischio di sicurezza cibernetica e di notifica di incidente **proporzionati**, anche in relazione al grado di esposizione dei soggetti a rischi, alle dimensioni dei soggetti stessi e alla probabilità che si verifichino incidenti, tenendo altresì conto della loro gravità e del loro impatto sociale ed economico.

Gli **obblighi** a cui si fa riferimento sono quelli di cui agli articoli 23, 24, 25, 27, 28 e 29, ossia: gli obblighi previsti nei confronti dei soggetti essenziali e importanti per la gestione dei rischi per la sicurezza informatica e per la notifica di incidente (articoli 23-25); gli obblighi eventuali ai soggetti essenziali e importanti relativi all'utilizzo di determinati prodotti TIC (tecnologie dell'informazione e della comunicazione), servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante (per la definizione di tali soggetti si rinvia alla scheda di lettura dell'articolo 6), ovvero da terze parti, purché siano certificati nell'ambito dei sistemi europei di certificazione della cibersicurezza (art. 27); gli obblighi in materia di specifiche tecniche per favorire l'attuazione efficace e armonizzata delle misure di gestione dei rischi di sicurezza cibernetica (art. 28), nonché quelli in relativi alla banca dei dati di registrazione dei nomi di dominio (art. 29).

Con una o più **determinazioni**, l'Agenzia, sentito il Tavolo per l'attuazione della disciplina NIS, istituito dall'articolo 12, stabilisce i termini (inclusa l'eventuale sospensione), le modalità e i tempi graduali di implementazione degli obblighi, differenziandoli anche in relazione alle categorie di rilevanza delle attività e dei servizi; al settore, al sottosettore e alla tipologia di soggetto; all'individuazione del soggetto quale essenziale o importante (**commi 2 e 3**).

Si ricorda in proposito che il **considerando 15 della direttiva NIS2**, sull'importanza di classificare i soggetti in due categorie, essenziali e importanti, prevede che i regimi di esecuzione e di vigilanza per tali due categorie di soggetti

dovrebbero essere differenziati per garantire un giusto equilibrio tra i requisiti e gli obblighi basati sui rischi, da un lato, e gli oneri amministrativi derivanti dalla vigilanza della conformità, dall'altro.

A ciò si aggiunge quanto previsto dal **considerando 81**, in base al quale "per evitare di imporre un onere finanziario e amministrativo sproporzionato ai soggetti essenziali e importanti, le misure di gestione dei rischi di cibersicurezza dovrebbero essere proporzionate ai rischi posti al sistema informatico e di rete interessato, tenendo conto dello stato dell'arte di tali misure e, se del caso, di pertinenti norme europee e internazionali, come anche dei relativi costi di attuazione".

Ai fini dell'attuazione degli obblighi, l'Agenzia può anche emanare **linee guida** vincolanti (**comma 4**) o **raccomandazioni** per supportare i soggetti nella loro implementazione (**comma 5**).

Il **comma 6** specifica che, per l'attuazione delle disposizioni in commento, l'Agenzia possa avvalersi dei **tavoli settoriali** previsti ai sensi dell'articolo 11, comma 4, del presente schema di decreto per contribuire all'efficace attuazione settoriale della direttiva nonché al relativo monitoraggio.

Infine, il **comma 7** dispone che le interazioni dei soggetti con l'Autorità nazionale competente NIS avvengono, in via prioritaria, per mezzo della piattaforma digitale **piattaforma digitale predisposta** dall'Agenzia ai sensi dell'articolo 7, comma 1.

Per approfondimenti si rinvia alle schede di lettura relative agli articoli richiamati.

Articolo 32
(Previsioni settoriali specifiche)

L'**articolo 32** prevede che l'Autorità nazionale competente NIS (cioè l'Agenzia per la cybersicurezza nazionale) possa imporre obblighi specifici a soggetti essenziali e importanti che forniscono servizi alla pubblica amministrazione. È previsto, inoltre, che alcuni enti possano essere esentati da specifici obblighi. Particolari esenzioni sono, poi, previste per i fornitori di servizi di registrazione dei nomi di dominio. Si prevede infine che, indipendente dalla designazione di un rappresentante nell'Unione europea, ai soggetti che offrono servizi nell'Unione, ma sono stabiliti fuori dalla stessa, si applichino gli obblighi di gestione del rischio per la sicurezza informatica e di notifica di incidente.

Il **comma 1** prevede che l'Agenzia per la cybersicurezza nazionale possa imporre specifici obblighi proporzionati e graduali ai soggetti essenziali e ai soggetti importanti (per la definizione dei quali si rinvia alla scheda di lettura dell'articolo 6) che forniscono servizi, anche digitali, alla pubblica amministrazione. Nel compiere tale operazione, l'Agenzia tiene conto degli impatti sociali ed economici di un incidente significativo nella catena di approvvigionamento del settore della pubblica amministrazione.

Secondo quanto disposto alla lettera *rr)* del comma 1 dell'articolo 2 del provvedimento in commento, per "**servizio digitale**" si intende qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.

Nel rinviare alla scheda dell'articolo 6 per approfondimenti, si ricorda che sono "**soggetti essenziali**":

- i soggetti operanti nei settori ad alta criticità indicati nell'allegato I che superano i massimali per le medie imprese (occupanti più di 249 persone e il cui fatturato annuo superi i 50 milioni di euro oppure il cui totale di bilancio annuo superi i 43 milioni di euro);
- i soggetti identificati come "soggetti critici" ai sensi del decreto legislativo, attualmente all'esame delle Camere (A.G. 165), che recepisce la direttiva (UE) 2022/2557, indipendentemente dalle loro dimensioni;
- i fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico aventi i requisiti dimensionali delle medie imprese;
- i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, indipendentemente dalle loro dimensioni;

- pubbliche amministrazioni centrali, indipendentemente dalle loro dimensioni (Organi costituzionali e di rilievo costituzionale, Presidenza del Consiglio dei ministri e Ministeri, Agenzie fiscali e Autorità amministrative indipendenti);
- i soggetti, indipendentemente dalle loro dimensioni, individuati dall'Autorità nazionale competente NIS nell'ambito: delle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III; dei soggetti delle tipologie di cui all'allegato IV (soggetti che forniscono servizi di trasporto pubblico locale, istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, società *in house*, società partecipate e società a controllo pubblico, come definite nel D.Lgs. n. 175/2016); dei soggetti delle tipologie di cui agli allegati I (settori ad alta criticità), II (settori critici) e IV (ulteriori tipologie di soggetti), indipendentemente dalle loro dimensioni, laddove soddisfino determinati requisiti; delle imprese collegate ad un soggetto essenziale o importante, se soddisfa determinati requisiti (art. 3, co. 10).

Sono "**soggetti importanti**" tutti i soggetti pubblici e privati che rientrano nell'ambito di applicazione del decreto (articolo 3) e che non sono considerati essenziali.

L'imposizione di specifici obblighi da parte dell'Agenzia ai soggetti essenziali e ai soggetti importanti che forniscono servizi, anche digitali, alla pubblica amministrazione avviene secondo le modalità di cui all'articolo 40, comma 5 del provvedimento in commento (e cioè con determinazioni dell'Agenzia) e fermo restando, comunque, quanto previsto agli articoli 23 (organi di amministrazione e direttivi), 24 (obblighi in materia di misure di gestione dei rischi per la sicurezza informatica), 25 (obblighi in materia di notifica di incidente), 27 (uso di schemi di certificazione della cybersicurezza), 28 (specifiche tecniche) e 29 (banca dei dati di registrazione dei nomi di dominio). Si rinvia sul punto alle relative schede di lettura.

In particolare, le modalità di cui all'articolo 40, comma 5, prevedono una determinazione dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS. Quest'ultimo, a norma dell'articolo 12: è costituito presso la citata Agenzia per la cybersicurezza nazionale; è presieduto dal direttore generale dell'Agenzia o da un suo delegato; è composto da un rappresentante di ogni Autorità di settore NIS e da due rappresentanti designati da regioni e province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano (si rinvia per approfondimenti alle schede degli articoli 11 e 12).

Il **comma 2** prevede che l'Agenzia, con propria determinazione e sentito il Tavolo per l'attuazione della disciplina NIS (istituito, come si è appena visto, dall'articolo 12 del provvedimento in esame), possa individuare, tra gli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente (capo IV), quelli che non si applicano:

- alle Città metropolitane, ai Comuni con popolazione superiore a 100.000 abitanti, ai Comuni capoluoghi di regione, alle Aziende sanitarie locali;
- agli Enti di regolazione dell'attività economica, agli Enti produttori di servizi economici, agli Enti a struttura associativa, agli Enti produttori di servizi assistenziali, ricreativi e culturali, agli Enti e le Istituzioni di ricerca, agli Istituti zooprofilattici sperimentali;
- ai soggetti delle tipologie di cui all'allegato IV del decreto, individuati secondo le procedure di cui al comma 13 dell'articolo 3 del provvedimento in commento. Si tratta, in particolare, dei soggetti che forniscono servizi di trasporto pubblico locale, degli istituti di istruzione che svolgono attività di ricerca, dei soggetti che svolgono attività di interesse culturale, delle società *in house*, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175. Le procedure di cui al comma 13 dell'articolo 3 prevedono l'individuazione da parte dell'Autorità nazionale competente NIS, su proposta delle Autorità di settore e sentito il Tavolo per l'attuazione della disciplina NIS. L'Agenzia per la cybersicurezza nazionale notifica quindi ai soggetti indicati la loro individuazione ai fini della registrazione sulla piattaforma digitale resa disponibile dalla stessa Agenzia (articolo 7, comma 1)
- al soggetto considerato critico, quale elemento sistemico della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti;
- indipendentemente dalle sue dimensioni, all'impresa collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri: a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale; b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale; c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale; d) fornisce servizi TIC (Tecnologie dell'informazione e della comunicazione) o di sicurezza, anche gestiti, al soggetto importante o essenziale.

Il **comma 3** prevede che gli obblighi in materia di misure di gestione dei rischi per la sicurezza informatica (articolo 24) e gli obblighi in materia di notifica di incidente (articolo 25) non si applichino ai soggetti che erogano esclusivamente servizi di registrazione dei nomi di dominio. Tali soggetti assicurano comunque un livello di sicurezza informatica coerente con gli obblighi anzidetti.

Si ricorda che, ai sensi della lettera *qq)* del comma 1 dell'articolo 2, per "**fornitore di servizi di registrazione di nomi di dominio**" si intende un *registrar*

o un agente che agisce per conto di *registrar*, come un fornitore o un rivenditore di servizi di registrazione per la *privacy* o di *proxy*.

Per effetto del **comma 4,** la designazione o la mancata designazione del rappresentante di cui all'articolo 5, comma 3, non pregiudica l'applicabilità degli obblighi di cui al capo IV (obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente).

Si ricorda che, a norma del comma 3 dell'articolo 5, qualora alcuni soggetti[11] non siano stabiliti nel territorio dell'Unione europea, ma offrano servizi all'interno dello stesso, essi designano un rappresentante nell'Unione europea. Tale rappresentante è stabilito in uno degli Stati membri in cui sono offerti i servizi ed è sottoposto alla relativa giurisdizione.

A norma del comma 4 in commento, quindi, anche ove manchi la designazione anzidetta, si applicano comunque gli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente.

[11] I fornitori di servizi di sistema dei nomi di dominio DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che sono sottoposti la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione. Si ricorda che, ai sensi del successivo comma 2, si considera stabilimento principale nell'Unione quello dello Stato membro nel quale sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio per la sicurezza informatica. Se non è possibile determinare lo Stato membro in cui sono adottate le suddette decisioni o se le stesse non sono adottate nell'Unione, lo stabilimento principale è considerato quello collocato nello Stato membro in cui sono effettuate le operazioni di sicurezza informatica, ovvero, ove ciò non sia possibile, quello dello Stato membro in cui il soggetto interessato ha lo stabilimento con il maggior numero di dipendenti nell'Unione europea.

Articolo 33
(Coordinamento con la disciplina del perimetro di sicurezza nazionale cibernetica)

L'**articolo 33** contiene disposizioni di coordinamento con la normativa nazionale relativa al Perimetro di sicurezza nazionale cibernetica in particolare per quel che concerne la disciplina sugli obblighi dei soggetti e dei loro rispettivi sistemi informativi, reti e servizi informatici.

L'**articolo 33** non si riferisce ad alcuna norma specifica della direttiva (UE) 2022/2555 ma risponde all'esigenza di coordinare lo schema di decreto in commento con la normativa vigente riguardo ad ambiti di esclusiva competenza nazionale. Nel caso specifico il collegamento è con il decreto legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 che istituisce il **Perimetro di sicurezza nazionale cibernetica** all'interno del quale vengono individuati soggetti pubblici e privati ai quali deve essere assicurato un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici in virtù della funzione essenziale che svolgono attraverso questi per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi nazionali e dal cui malfunzionamento, interruzione o utilizzo improprio, può derivare un pregiudizio per la sicurezza nazionale (**articolo 1, comma 2, lettera b)**). Il decreto legge attiene, dunque, direttamente agli interessi nazionali e alla tutela della sicurezza nazionale che rientrano nei casi di esclusiva responsabilità dello Stato come riportato dall'**articolo 4** dello schema di decreto in commento.

Il **comma 1**, infatti, reca che, proprio ai fini del medesimo **articolo 4**:

a) gli obblighi di gestione del rischio per la sicurezza informatica e di notifica di incidente previsti dal decreto legge di cui sopra sono considerati almeno equivalenti a quelli previsti dallo schema di norma in commento;
b) non si applicano le disposizioni del medesimo schema di decreto alle reti, ai sistemi informativi e ai servizi informatici da cui, come reca l'**articolo 1, comma 2, lettera b) del decreto legge n. 105/2019**, dipende l'esercizio delle funzioni essenziali in relazioni alle quali i soggetti vengono inseriti nel Perimetro;
c) i soggetti individuati ai sensi del **comma 2, lettera a)**, **del decreto legge n. 105/2019** – sulla base delle funzioni essenziali esercitate

attraverso reti, sistemi informativi e servizi informatici e in virtù di ciò registrati, ai sensi dell'**articolo 1, comma 2 bis**, della medesima disposizione in un atto amministrativo che viene adottato dal Presidente del Consiglio dei ministri, su proposta del **Comitato interministeriale per la cybersicurezza (CIC)** – non sono sottoposti agli obblighi di notificare al **CSIRT Italia** gli incidenti che abbiano un impatto significativo che, ai sensi dell'**articolo 25** dello schema di decreto, sono quelli recanti una grave disfunzione o perdite finanziarie oppure che comportano o possono comportare ripercussioni su altre persone fisiche o giuridiche o causare perdite materiali o immateriali, limitatamente agli ambiti di applicazione dell'**articolo 1, comma 3 del decreto legge n. 105/2019**, ovvero se colpiscono reti, sistemi informativi e servizi informatici.

Si ricorda che il **CIC** è istituito dall'**articolo 4** del decreto legge del 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) presso la Presidenza del Consiglio dei ministri con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza. Il **CSIRT Italia**, invece, è trasferito presso l'Agenzia per la cybersicurezza nazionale (*infra*) dallo stesso **decreto legge n.82 del 2021** e risponde all'obbligo, di cui **all'articolo 1, paragrafo 2 lettera a)**, **della direttiva (UE) 2022/2555,** per ciascuno Stato membro di istituire un organo preposto alle funzioni di gestione degli incidenti di sicurezza. In precedenza il CSIRT Italiano, era istituito presso la Presidenza del Consiglio dei Ministri dal decreto legislativo 18 maggio 2018, n. 65 (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).

d) Le informazioni attinenti ai soggetti di cui alla lettera precedente o quelle da loro trasmesse all'Agenzia per la cybersicurezza nazionale possono essere escluse dagli obblighi di comunicazione che quest'ultima deve rendere alla Commissione europea ai sensi dell'**articolo 22** dello schema di decreto.

L'**Agenzia per la cybersicurezza** nazionale è istituita dall'**articolo 5 del decreto legge n.82 del 2021** sopra citato a tutela degli interessi nazionali nel campo di riferimento. L'**articolo 7** ne determina le funzioni, ovvero, in particolare la predisposizione della Strategia nazionale di cibersicurezza (*per approfondimenti si rimanda alla scheda relativa all'articolo 9*), l'assunzione dei compiti precedentemente attribuiti a diversi soggetti, quali il Ministero dello sviluppo economico, la Presidenza del Consiglio, il Dipartimento delle informazioni e della sicurezza, l'Agenzia per l'Italia digitale e la promozione di iniziative per lo sviluppo di competenze e capacità.

CAPO V – MONITORAGGIO, VIGILANZA ED ESECUZIONE

Articolo 34
(Principi generali per lo svolgimento delle attività di vigilanza ed esecuzione)

L'**articolo 34** attribuisce all'Agenzia per la cybersicurezza nazionale, in quanto Autorità nazionale competente NIS, i compiti di monitoraggio del rispetto degli obblighi previsti dal provvedimento per i "soggetti essenziali" e per i "soggetti importanti"

Per la definizione di "soggetti essenziali" e "soggetti importanti" si rinvia alle schede di lettura dell'articolo 6.

Il **comma 1** precisa poi che nello specifico si tratta del rispetto degli obblighi previsti:

- dall'articolo 7 vale a dire iscrizione negli appositi elenchi e fornitura delle informazioni previste da tale articolo (quali ad esempio lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso o nella disponibilità del soggetto; l'elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione del provvedimento);
- dal Capo IV (articoli da 23 a 33) del provvedimento relativo agli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente; si tratta, tra gli altri, dell'obbligo di adottare misure tecniche, operative e organizzative adeguate e proporzionate per la gestione dei rischi (articolo 24) e dell'obbligo di notifica di un incidente (articolo 25).

Il comma 1 afferma che le attività di vigilanza saranno svolte attraverso:

- il monitoraggio, l'analisi e il supporto;
- la verifica e le ispezioni;
- l'adozione di misure di esecuzione;
- l'irrogazione di sanzioni amministrative pecuniarie e accessorie

Il **comma 2** stabilisce che l'Agenzia può attribuire priorità ad alcune delle attività sopra richiamate "adottando un approccio basato sul rischio", vale a dire, sembra desumersi, sulla base del livello di rischio.

In base ai commi successivi:

- le attività di vigilanza svolte dall'Agenzia dovranno essere effettive, proporzionate e dissuasive (**comma 3**);
- l'Agenzia dovrà operare con indipendenza operativa rispetto agli enti della pubblica amministrazione sottoposti a vigilanza (**comma 4**);
- l'Agenzia dovrà motivare i suoi provvedimenti (**comma 5**);
- l'Agenzia svolgerà i suoi compiti nel rispetto dei diritti della difesa e tenendo conto, tra le altre cose, della gravità della violazione (con riferimento, tra le altre cose, alla ripetizione delle violazioni o alla mancata notifica di incidenti significativi o ancora all'ostacolo alle attività di vigilanza); della sua durata; delle eventuali precedenti violazioni; di qualsiasi danno materiale o immateriale causato; dell'eventuale condotta intenzionale o negligenza (**comma 6**);
- gli audit sulla sicurezza previsti dagli articoli 35 e 37 (sul punto si rinvia alle relative schede di lettura) saranno svolti da organismi indipendenti e si baseranno su valutazioni del rischio effettuate dall'Agenzia o dal soggetto sottoposto ad audit o su altre informazioni disponibili in relazione ai rischi (**comma 7**);
- se i fornitori di servizi di sistema dei nomi di dominio DNS stabiliti fuori dal territorio dell'Unione non designeranno un loro rappresentante nell'Unione ai sensi dell'articolo 5, comma 3, del provvedimento in esame, questo comunque non pregiudicherà lo svolgimento dei compiti di vigilanza dell'Agenzia (**comma 8**) ;
- le comunicazioni tra l'Agenzia e i soggetti essenziali ed importanti avverranno attraverso la piattaforma digitale prevista dall'articolo 7, per la quale si rinvia alla relativa scheda di lettura (**comma 9**).

Il **comma 10**, infine, rimette a un DPCM la definizione di criteri e modalità per lo svolgimento delle attività di vigilanza.

Articolo 35
(Monitoraggio, analisi e supporto)

L'**articolo 35** prevede una serie di **obblighi di monitoraggio, analisi e supporto** in capo all'Agenzia per la cybersicurezza nazionale in quanto **Autorità nazionale competente NIS**.

Ai fini di quanto dispone l'articolo 7 in merito alla identificazione ed elencazione dei soggetti essenziali e dei soggetti importanti, al **comma 1** dell'articolo 35 si stabilisce che l'Agenzia **verifica** e fornisce riscontro circa le **informazioni** trasmesse e la relativa corrispondenza ai requisiti prescritti per i soggetti registrati, ai fini dell'inserimento nell'**elenco dei soggetti essenziali e dei soggetti importanti** (per i quali si rinvia alla scheda di lettura dell'articolo 6) assicurando altresì adeguata pubblicità ai criteri concernenti l'ambito di applicazione del presente decreto e dei relativi obblighi.

Secondo il **comma 2**, l'Agenzia monitora l'attuazione degli obblighi previsti dal decreto in esame da parte dei soggetti che rientrano nel suo ambito di applicazione, implementando, altresì, interventi di supporto per i soggetti medesimi.

Al **comma 3** si prevede che, ai fini dell'attività di monitoraggio di cui al comma 2, la medesima Agenzia può:

a) richiedere ai soggetti una rendicontazione, anche periodica, ivi incluse autovalutazioni e piani di implementazione, dello stato di attuazione degli obblighi di cui al provvedimento in esame, nonché le informazioni necessarie per lo svolgimento dei propri compiti istituzionali, dichiarando la finalità della richiesta;

b) richiedere ai soggetti l'esecuzione, periodica o mirata, di audit sulla sicurezza, in particolare in caso di incidente significativo o di violazione del presente decreto da parte del soggetto;

c) richiedere ai soggetti l'esecuzione di scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;

d) emanare raccomandazioni e avvertimenti relativi a presunte violazioni del presente decreto da parte dei soggetti interessati.

Ai fini del comma 2, l'Agenzia indica modalità e termini ragionevoli e proporzionati per adempiere, nonché per riferire circa lo stato di attuazione degli adempimenti (**comma 4**).

Le risultanze delle attività di cui al presente capo sono analizzate dall'Agenzia stessa al fine di stabilire l'ordine di priorità degli interventi di supporto di cui al comma 2 nonché di individuare gli indirizzi di sviluppo della regolamentazione di cui all'articolo 31 (**comma 5;** sul punto si rinvia alla scheda di lettura dell'articolo 31). Qualora ciò non costituisca un onere sproporzionato o eccessivo, è la medesima Autorità nazionale competente NIS a implementare gli interventi di supporto di cui al comma 2 (**comma 6**).

Nello svolgimento delle attività di cui al capo in esame, l'Autorità si può avvalere dei tavoli settoriali di cui all'articolo 11, comma 4, lettera f) (**comma 7**).

Articolo 36
(Verifiche e ispezioni)

L'**articolo 36** prevede che l'Agenzia per la cybersicurezza nazionale, in qualità di autorità nazionale competente NIS possa effettuare verifiche documentali, ispezioni *in loco* e a distanza, e richiedere dati e informazioni ai soggetti rientranti nell'ambito di applicazione del decreto. Tali poteri possono essere esercitati nei confronti dei soggetti importanti solo qualora ci siano prove o indicazioni di possibili violazioni del decreto.

L'articolo 36 consta di due commi e recepisce alcune disposizioni contenute all'articolo 32 della direttiva 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022.

Il **comma 1** prevede che l'Agenzia, nell'esercizio dei poteri di verifica e ispettivi nei confronti dei soggetti che rientrano nell'ambito di applicazione del decreto in commento, possa sottoporre questi ultimi a verifiche, ispezioni e richieste di accesso ad informazioni.

Si rinvia alla scheda dell'articolo 3 per l'individuazione dei soggetti ai quali si applica il decreto.

In particolare, la **lettera *a)*** dispone che l'Autorità citata possa procedere a verifiche della documentazione e delle informazioni trasmesse all'Autorità stessa in ottemperanza alle disposizioni del decreto.

La lettera *b)* prevede che l'Autorità possa ispezionare in loco e a distanza i soggetti rientranti nell'ambito di applicazione del decreto. Tra tali ispezioni rientrano i controlli casuali.

La **lettera *c)*** stabilisce che l'Autorità possa sottoporre i soggetti citati a richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei poteri di verifica e ispezione. Nel compiere tale procedura, l'Autorità deve dichiarare la finalità della richiesta e specificare le informazioni pretese.

Il **comma 2** dispone che, nei confronti dei soggetti importanti, i poteri di verifica e ispettivi si applichino solo se l'Autorità nazionale competente NIS acquisisca o riceva elementi di prova, indicazioni o informazioni che suggeriscano possibili violazioni del decreto in commento.

Nel rinviare alla scheda dell'articolo 6 per approfondimenti, si ricorda che sono "**soggetti importanti**" tutti i soggetti pubblici e privati che rientrano nell'ambito di applicazione del decreto (articolo 3) e che non sono considerati **essenziali**.

Sono "soggetti essenziali":

- i soggetti operanti nei settori ad alta criticità indicati nell'allegato I che superano i massimali per le medie imprese (occupanti più di 249 persone e il cui fatturato annuo superi i 50 milioni di euro oppure il cui totale di bilancio annuo superi i 43 milioni di euro);
- i soggetti identificati come "soggetti critici" ai sensi del decreto legislativo, attualmente all'esame delle Camere (A.G. 165), che recepisce la direttiva (UE) 2022/2557, indipendentemente dalle loro dimensioni;
- i fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico aventi i requisiti dimensionali delle medie imprese;
- i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, indipendentemente dalle loro dimensioni;
- pubbliche amministrazioni centrali, indipendentemente dalle loro dimensioni (Organi costituzionali e di rilievo costituzionale; è però escluso il Parlamento; Presidenza del Consiglio dei ministri e Ministeri, Agenzie fiscali e Autorità amministrative indipendenti);
- i soggetti, indipendentemente dalle loro dimensioni, individuati dall'Autorità nazionale competente NIS nell'ambito: delle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III; dei soggetti delle tipologie di cui all'allegato IV (soggetti che forniscono servizi di trasporto pubblico locale, istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, società *in house*, società partecipate e società a controllo pubblico, come definite nel D.Lgs. n. 175/2016); dei soggetti delle tipologie di cui agli allegati I (settori ad alta criticità), II (settori critici) e IV (ulteriori tipologie di soggetti), indipendentemente dalle loro dimensioni, laddove soddisfino determinati requisiti; delle imprese collegate ad un soggetto essenziale o importante, se soddisfa determinati requisiti (art. 3, co. 10).

Articolo 37
(Misure di esecuzione)

L'**articolo 37** individua le misure di esecuzione che l'Agenzia per la cybersicurezza nazionale in quanto Autorità nazionale competente NIS può assumere. In particolare, l'Autorità può intimare di eseguire alcuni adempimenti ai soggetti interessati. L'articolo dispone in merito al procedimento per lo svolgimento delle misure di esecuzione: vi è una prima fase dedicata alla notifica delle conclusioni preliminari; vi è quindi la possibilità di controdedurre da parte dei soggetti interessati; l'Autorità procede poi all'intimazione dei comportamenti da tenere; si prevede infine, in caso di mancata ottemperanza, la diffida ad adempiere. Misure specifiche sono previste per i provvedimenti urgenti.

L'articolo 37 consta di dieci commi e recepisce alcune disposizioni contenute all'articolo 32 della direttiva 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022.

Il **comma 1** prevede che l'Agenzia per la cybersicurezza nazionale, ai fini dell'esercizio dei suoi poteri di esecuzione, tenga anche conto degli esiti delle attività di monitoraggio, analisi e supporto di cui all'articolo 35. L'autorità, per le stesse finalità, deve tener conto, altresì, delle risultanze dell'esercizio dei poteri di verifica e ispettivi di cui all'articolo 36.

Con riferimento all'**attività di monitoraggio, analisi e supporto**, si ricorda che, ai sensi dell'articolo 35 del decreto, ai fini dell'identificazione ed elencazione dei soggetti essenziali e dei soggetti importanti, l'Autorità nazionale competente NIS verifica le informazioni trasmesse dai soggetti registrati, assicurandosi che rispettino i requisiti prescritti, e pubblicizza i criteri relativi all'ambito di applicazione e agli obblighi del decreto. L'Autorità monitora l'adempimento degli obblighi da parte dei soggetti ai quali si applicano le disposizioni del decreto e fornisce supporto agli stessi. Con riferimento all'attività di monitoraggio, l'autorità nazionale competente NIS può: richiedere rendicontazioni periodiche, autovalutazioni e piani di implementazione degli obblighi del decreto; richiedere audit sulla sicurezza, specialmente in caso di incidenti significativi o violazioni del decreto; richiedere scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti; emanare raccomandazioni e avvertimenti su presunte violazioni del decreto da parte dei soggetti interessati. Con riferimento all'analisi, l'Autorità esamina i risultati delle attività per stabilire le priorità degli interventi di supporto e individuare gli indirizzi di sviluppo della regolamentazione.

In relazione all'esercizio dei **poteri di verifica e ispettivi**, si ricorda che, ai sensi dell'articolo 36 del decreto, l'Autorità nazionale competente NIS: verifica la documentazione e le informazioni a essa trasmesse dai soggetti cui si applica il decreto; sottopone questi ultimi a ispezioni in loco e a distanza, compresi controlli casuali; può richiedere ai soggetti anzidetti l'accesso a dati, documenti e altre informazioni necessarie, specificando lo scopo della richiesta e le informazioni richieste. Per i soggetti considerati importanti, i poteri di verifica e ispezione si applicano solo se l'Autorità ha prove, indicazioni o informazioni che suggeriscano possibili violazioni del decreto.

Il **comma 2** prevede che l'Agenzia per la cybersicurezza nazionale, nell'esercizio dei suoi poteri di esecuzione, possa richiedere ai soggetti, dichiarandone la finalità, di fornire i dati che dimostrino l'attuazione di politiche di sicurezza informatica, quali i risultati di audit sulla sicurezza e i relativi elementi di prova, nonché le informazioni necessarie per lo svolgimento dei propri compiti istituzionali.

Nel rinviare alla scheda dell'articolo 2 per approfondimenti, si ricorda che per "**audit**" (lettera *nnn)*, comma 1, articolo 2) si intende l'attività di verifica, a distanza o in loco, sistematica, documentata e indipendente che ha come scopo quello di vagliare la corrispondenza agli obblighi di cui al capo IV del decreto in commento (obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente), effettuata da un organismo indipendente qualificato o dall'Autorità nazionale competente NIS.

Secondo quanto disposto alla **lettera *a)*** del comma 2, l'anzidetta richiesta di dati e informazioni può essere effettuata dall'Autorità, anche ai fini della valutazione delle misure di gestione dei rischi per la sicurezza informatica.

Ai sensi della lettera *r)*, per "**sicurezza informatica**" si intende l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche.

La **lettera *b)*** del comma 2 prevede che la richiesta di dati e informazioni possa avvenire anche ai fini del rispetto degli obblighi di trasmissione, comunicazione e notifica di cui al decreto in commento.

Il **comma 3** dispone che l'Agenzia per la cybersicurezza nazionale, nell'esercizio dei suoi poteri di esecuzione, possa intimare ai soggetti di eseguire alcuni adempimenti.

In particolare, la **lettera *a)*** del comma 3 prevede che ai soggetti possa essere intimato di eseguire, su base periodica o mirata, audit sulla sicurezza, in particolare in caso di incidente significativo o di violazione del decreto in

commento da parte del soggetto. Si prevede, inoltre, che l'Agenzia non possa prescrivere l'esecuzione periodica di audit di sicurezza ai soggetti importanti.

Nel rinviare alla scheda dell'articolo 6 per approfondimenti, si ricorda che sono "**soggetti importanti**" tutti i soggetti pubblici e privati che rientrano nell'ambito di applicazione del decreto (articolo 3) e che non sono considerati **essenziali**.

Sono "soggetti essenziali":

- i soggetti operanti nei settori ad alta criticità indicati nell'allegato I che superano i massimali per le medie imprese (occupanti più di 249 persone e il cui fatturato annuo superi i 50 milioni di euro oppure il cui totale di bilancio annuo superi i 43 milioni di euro);
- i soggetti identificati come "soggetti critici" ai sensi del decreto legislativo, attualmente all'esame delle Camere (A.G. 165), che recepisce la direttiva (UE) 2022/2557, indipendentemente dalle loro dimensioni;
- i fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico aventi i requisiti dimensionali delle medie imprese;
- i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, indipendentemente dalle loro dimensioni;
- pubbliche amministrazioni centrali, indipendentemente dalle loro dimensioni (Organi costituzionali e di rilievo costituzionale, con esclusione del Parlamento; Presidenza del Consiglio dei ministri e Ministeri, Agenzie fiscali e Autorità amministrative indipendenti);
- i soggetti, indipendentemente dalle loro dimensioni, individuati dall'Autorità nazionale competente NIS nell'ambito: delle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III; dei soggetti delle tipologie di cui all'allegato IV (soggetti che forniscono servizi di trasporto pubblico locale, istituti di istruzione che svolgono attività di ricerca, soggetti che svolgono attività di interesse culturale, società *in house*, società partecipate e società a controllo pubblico, come definite nel D.Lgs. n. 175/2016); dei soggetti delle tipologie di cui agli allegati I (settori ad alta criticità), II (settori critici) e IV (ulteriori tipologie di soggetti), indipendentemente dalle loro dimensioni, laddove soddisfino determinati requisiti; le imprese collegate ad un soggetto essenziale o importante, se soddisfa determinati requisiti (art. 3, co. 10).

La **lettera *b)*** del comma 3 prevede che ai soggetti possa essere intimato dall'Autorità di eseguire scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con la medesima Autorità.

Secondo quanto disposto dalla **lettera *c)***, l'Autorità può intimare ai soggetti di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza.

Ai sensi della **lettera *d)***, l'intimazione può avere ad oggetto l'adempimento degli obblighi contenuti nel decreto in commento.

Ai soggetti può essere intimato di porre termine al comportamento che viola il presente decreto e di astenersi dal ripeterlo (**lettera *e)***;

La **lettera *f)*** prevede che l'Autorità possa intimare ai soggetti di attuare le istruzioni vincolanti impartite dalla medesima Autorità o di porre rimedio alle carenze individuate nell'adempimento degli obblighi di cui al decreto in commento o alle conseguenze che derivano da violazioni dello stesso.

La **lettera *g)*** dispone che ai soggetti possa essere intimato, ai fini del comma 9 dell'articolo 25 del decreto, di comunicare senza ingiustificato ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.

Si ricorda che, nell'ambito della più ampia materia di obblighi relativi alla notifica di incidente, il comma 9 dell'articolo 25 prescrive che sentito il CSIRT Italia (il Gruppo nazionale di risposta agli incidenti di sicurezza informatica), se ritenuto opportuno e qualora possibile, i soggetti essenziali e i soggetti importanti comunicano, senza ingiustificato ritardo, ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.

Ai sensi della **lettera *h)***, ai fini del comma 10 dell'articolo 25, può essere intimato ai soggetti di comunicare senza ingiustificato ritardo ai destinatari dei loro servizi, che sono potenzialmente interessati da una minaccia informatica significativa, qualsiasi misura o azione correttiva che tali destinatari possono adottare in risposta a tale minaccia, nonché, se opportuno, la minaccia informatica significativa stessa.

In proposito, il comma 10 dell'articolo 25 dispone che i soggetti essenziali e i soggetti importanti, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, comunicano senza ingiustificato ritardo, ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa, misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia. Inoltre, sentito il CSIRT Italia, se ritenuto opportuno, i soggetti essenziali e i soggetti importanti comunicano ai medesimi destinatari anche la natura di tale minaccia informatica significativa.

Si ricorda che per "**minaccia informatica**" si intende qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e su altre persone (articolo 2, comma 1, lettera *bb*).

La lettera *cc)* del comma 1 dell'articolo 2 del decreto in commento prevede che per "**minaccia informatica significativa**" si intenda una minaccia informatica che,

in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informativi e di rete di un soggetto o sugli utenti dei servizi erogati da un soggetto causando perdite materiali o immateriali considerevoli.

La **lettera *i)*** prevede che l'Autorità possa intimare ai soggetti di informare il pubblico sugli incidenti occorsi.

In proposito, il comma 11 dell'articolo 25 prevede che l'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, anche sentendo, se del caso, le autorità competenti e i CSIRT nazionali degli altri Stati membri interessati, possa informare il pubblico riguardo all'incidente significativo per evitare ulteriori incidenti significativi o per gestire un incidente significativo in corso, o qualora ritenga che la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico.

Si ricorda che per "**incidente**" si intende un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi (articolo 2, comma 1, lettera *t*)

Ai sensi della **lettera *l)***, l'Autorità può intimare ai soggetti di rendere pubbliche le violazioni di cui al decreto in commento.

Il **comma 4** dispone che l'Agenzia per la cybersicurezza nazionale, in quanto Autorità nazionale competente NIS, possa intimare l'osservanza di istruzioni vincolanti al fine di evitare il verificarsi di un incidente o per porvi rimedio.

Il **comma 5** prevede che l'Agenzia per la cybersicurezza nazionale possa designare un proprio funzionario per supportare il soggetto interessato ai fini dell'adempimento degli obblighi di cui allo schema di decreto in commento. È previsto che tale funzionario sia investito di compiti ben definiti nell'arco di un periodo di tempo determinato, anche tramite visite in loco e a distanza. Si prevede, inoltre, che il soggetto interessato assicuri la piena collaborazione con il funzionario designato.

Il **comma 6** stabilisce che, qualora il soggetto interessato non adempia alle disposizioni di cui ai commi 2, 3, 4 e 5, secondo periodo, del presente articolo, l'Agenzia per la cybersicurezza nazionale diffidi il soggetto ad adempiere a tali disposizioni.

Il **comma 7** dispone che, ai fini dei commi 2, 3, 4 e 6 (ossia le intimazioni e la diffida previste dal presente articolo), l'Autorità indichi modalità e termini ragionevoli e proporzionati per adempiere nonché per riferire circa lo stato di attuazione degli adempimenti.

Il **comma 8** prevede che, prima di adottare provvedimenti di cui ai commi 3 (intimazioni) e 6 (diffida), l'Agenzia notifichi ai soggetti interessati le conclusioni preliminari, concedendo a questi ultimi un termine ragionevole, comunque non inferiore a quindici giorni, per presentare osservazioni. Tale disposizione, a norma di quanto previsto al successivo **comma 9,** non trova applicazione nei casi in cui la notifica delle conclusioni preliminari non consenta azioni immediate per prevenire un incidente o rispondervi (si tratta, sostanzialmente, dei casi di urgenza). In tale eventualità è previsto che l'Agenzia motivi l'omissione della notifica. Al **comma 10** è poi previsto che, nei casi di adozione da parte dell'Agenzia di più provvedimenti successivi riconducibili alla medesima fattispecie (più intimazioni o diffide per lo stesso fatto), la notifica delle conclusioni preliminari ai soggetti interessati con la concessione a questi ultimi del termine per presentare osservazioni (comma 8) sia disposta esclusivamente con riferimento al primo di questi provvedimenti.

Articolo 38
(Sanzioni amministrative)

L'**articolo 31** disciplina l'**autorità competente**, le **fattispecie** oggetto di **sospensione** dell'attività e quelle passibili di **sanzione** amministrativa in violazione delle disposizioni del provvedimento in esame, il regime della **reiterazione** delle violazioni, gli **strumenti deflattivi del contenzioso** e la **destinazione dei proventi** delle sanzioni amministrative.

Ai sensi del **comma 1** l'Agenzia per la cybersicurezza nazionale in quantoAutorità nazionale competente NIS, è competente alla irrogazione delle sanzioni amministrative, e a tal fine tiene anche conto degli esiti delle attività di monitoraggio, supporto e analisi, delle risultanze dell'esercizio dei suoi poteri di verifica e ispettivi all'articolo 36, nonché dell'esercizio dei poteri di esecuzione di cui all'articolo 37 (si veda la scheda sull'articolo precedente).

L'Agenzia per la cybersicurezza nazionale (ACN) con proprie determinazioni, sentito il Tavolo attuazione NIS istituito dall'articolo 12, può specificare laddove necessario i criteri per la determinazione dell'importo delle sanzioni per le violazioni, e adottare le misure necessarie per assicurarne l'effettività, la proporzionalità, la dissuasività e l'applicazione (**comma 2**).

La disciplina del meccanismo sanzionatorio, oggetto dell'articolo in esame, è strettamente connesso con quella delle misure di esecuzione di cui al precedente articolo 37. L'ACN, nell'esercizio dei suoi poteri di esecuzione di cui al citato articolo 37, può richiedere, a seguito di verifiche e ispezioni, ai soggetti che rientrano nell'ambito di applicazione della direttiva oggetto di recepimento di fornire informazioni o di adempiere a specifichi obblighi (art. 37, commi 2-5). In caso di inadempienza, l'ACN diffida il soggetto ad adempiere entro un dato termine (art. 37, commi 6 e 7).

Se anche dopo il decorso di tale termine le inadempienze permangono, l'ACN può sospendere l'attività del soggetto (art. 38, commi 4-7).

L'applicazione esercizio dei poteri di esecuzione (di cui all'articolo 37) non impedisce la contestazione delle violazioni e la relativa irrogazione di sanzioni amministrative (**comma 3** dell'articolo 38 in esame).

Come anticipato sopra, i **commi da 4 a 7** prevedono un sistema di sanzioni basate sulla **sospensione delle attività** in caso di inadempienza ad ottemperare alle diffide dell'ACN. La sospensione delle attività riguarda sia

persone giuridiche (**comma 4**), sia le persone fisiche (**commi 5 e 6**), quali dirigenti e rappresentanti legali. Per quest'ultimi la sanzione comporta la incapacità di svolgere funzioni dirigenziali presso il soggetto interessato. La sospensione non viene applicata nei confronti delle pubbliche amministrazioni e dei soggetti partecipati o sottoposti a controllo pubblico (comma 4, ultimo periodo), né nei confronti dei dipendenti pubblici per i quali si applicano le norme in materia di responsabilità dei dipendenti pubblici e dei funzionari e può costituire causa di responsabilità disciplinare e amministrativo contabile (**comma 7**).

Per quanto riguarda la responsabilità dirigenziale, l'articolo 21 del D.lgs. 165/2001 richiama il mancato raggiungimento degli obiettivi, accertato attraverso le risultanze del sistema di valutazione, e l'inosservanza delle direttive imputabili al dirigente quali elementi che comportano, previa contestazione l'impossibilità di rinnovo dell'incarico dirigenziale. In relazione alla gravità dei casi, l'amministrazione può inoltre, previa contestazione e nel rispetto del principio del contraddittorio, revocare prima della scadenza l'incarico collocando il dirigente a disposizione dei ruoli delle amministrazioni dello Stato ovvero recedere dal rapporto di lavoro secondo le disposizioni del contratto collettivo (comma 1).

Resta ferma l'eventuale responsabilità disciplinare secondo la disciplina contenuta nel contratto collettivo.

Inoltre, nel caso di colpevole omessa vigilanza sull'effettiva produttività delle risorse umane assegnate e sull'efficienza della struttura dipendente dal dirigente: la sanzione consiste nella decurtazione della retribuzione di risultato (comma 1-*bis*).

La responsabilità amministrativo-contabile si configura qualora il dipendente pubblico (o soggetto legato alla p.a. da rapporto di servizio), per inosservanza dolosa o gravemente colposa dei propri obblighi di servizio, provochi un danno alla propria amministrazione o ad altro ente pubblico.

Con riferimento alle singole **fattispecie oggetto di sanzione**, previste dai **commi da 8 a 11**, dell'articolo in esame, si rinvia alla trattazione delle medesime effettuata per le specifiche disposizioni alle quali le singole sanzioni afferiscono.

La direttiva NIS 2 oggetto di recepimento (artt. 34 e 36) prevede, a questo riguardo, che gli Stati membri stabiliscano le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della medesima adottando tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste sono effettive, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.

Gli Stati membri notificano tali norme e provvedimenti alla Commissione entro il 17 gennaio 2025 e provvedono a darle immediata notifica di ogni successiva modifica.

In termini generali le sanzioni individuate per la violazione degli obblighi previsti in capo agli operatori di servizi essenziali e ai fornitori di servizi

digitali variano tra un minimo di 10 mila euro ad un massimo di 10 milioni di euro e (per i soggetti diverse delle pubbliche amministrazioni) tra un minimo dello 0,07% ed un massimo del 2% del fatturato annuo su scala mondiale.

Il **comma 12** prevede che in caso di **reiterazione** non specifica la sanzione prevista è aumentata fino al triplo, mentre in caso di violazione specifica la sanzione è aumentata fino al doppio.

Secondo quanto previsto dall'articolo 8-*bis* della legge n. 689 del 1981 si ha reiterazione quando, nei cinque anni successivi alla commissione di una violazione amministrativa, accertata con provvedimento esecutivo, lo stesso soggetto commette un'altra violazione della stessa indole. Si ha reiterazione anche quando più violazioni della stessa indole commesse nel quinquennio sono accertate con unico provvedimento esecutivo. Per violazioni della stessa indole si intendono le violazioni della medesima disposizione e quelle di disposizioni diverse che, per la natura dei fatti che le costituiscono o per le modalità della condotta, presentano una sostanziale omogeneità o caratteri fondamentali comuni. La reiterazione è specifica se è violata la medesima disposizione.

Quanto alle procedure applicabili all'accertamento e all'irrogazione delle sanzioni si applicano le disposizioni contenute nel capo I, sezioni I e II, della legge n. 689 del 1981.

In base alla **legge n. 689 del 1981** *(Modifiche al sistema penale)*, l'applicazione della sanzione amministrativa pecuniaria avviene secondo il seguente procedimento:

- **accertamento** da parte degli organi di controllo competenti o della polizia giudiziaria (art. 13),
- **contestazione** immediata al trasgressore o notifica entro 90 giorni;
- **pagamento in misura ridotta** entro i successivi 60 giorni (pari alla terza parte del massimo previsto o al doppio del minimo) **o inoltro**, entro 30 giorni, **di memoria difensiva all'autorità competente**, che decide se procedere all'archiviazione o all'emanazione di un'ordinanza-ingiunzione di pagamento;
- eventuale **opposizione all'ordinanza-ingiunzione**, entro 30 giorni dalla sua notificazione, davanti all'autorità giudiziaria competente, ovvero il giudice di pace a meno che, per il valore della controversia (sanzione pecuniaria superiore nel massimo a 15.493 euro) o per la materia trattata (tutela del lavoro, igiene sui luoghi di lavoro e prevenzione degli infortuni sul lavoro; previdenza e assistenza obbligatoria; tutela dell'ambiente dall'inquinamento, della flora, della fauna e delle aree protette; igiene degli alimenti e delle bevande; materia valutaria; antiriciclaggio), non sussista la competenza del tribunale). L'esecuzione dell'ingiunzione non viene sospesa e il giudizio che con esso si instaura si può concludere o con un'ordinanza di convalida del provvedimento o con sentenza di annullamento o modifica del provvedimento. Il giudice ha piena facoltà

sull'atto, potendo o annullarlo o modificarlo, sia per vizi di legittimità che di merito;
- **accoglimento dell'opposizione**, anche parziale, **o rigetto**: il giudice ha piena facoltà sull'atto, potendo o annullarlo o modificarlo, sia per vizi di legittimità che di merito (sentenza ricorribile per cassazione);
- decorso il termine fissato dall'ordinanza-ingiunzione, in assenza del pagamento, eventuale **esecuzione forzata** per la riscossione delle somme in base alle norme previste per l'esazione delle imposte dirette.

Il termine di **prescrizione** delle sanzioni amministrative pecuniarie è di **5 anni** dal giorno della commessa violazione.

I **commi 13 e 14** individuano due tipologie particolari di violazione:

mancata o tardiva registrazione nella piattaforma digitale da parte dei soggetti essenziali e dei soggetti importanti (di cui all'articolo 7): si applica la sanzione prevista per la violazione più grave aumentata fino al triplo;

mancata osservanza degli obblighi relativi alla notifica di incidente: le sanzioni si applicano solo in caso di reiterazione specifica nell'arco di cinque anni e l'Autorità nazionale competente NIS può esercitare, durante i dodici mesi successivi all'accertamento della violazione, i poteri di verifica e ispettivi.

Con DPCM, adottato ai sensi dell'articolo 40, comma 1, lettera c), sono disciplinate le modalità di applicazione, nell'ambito del procedimento sanzionatorio, dei strumenti deflattivi del contenzioso (**comma 15**):

- invito a conformarsi che l'ACN - l'Autorità nazionale competente NIS, ove accerti la sussistenza delle violazioni, e fatto salvo il caso di reiterazione delle stesse, invia al trasgressore, assegnando un congruo termine perentorio, proporzionato al tipo e alla gravità della violazione, per conformare la condotta agli obblighi previsti dalla normativa vigente.
- facoltà di estinguere il procedimento attraverso il pagamento in misura ridotta pari alla terza parte del massimo della sanzione o se più favorevole, e qualora sia stabilito, al doppio del minimo della sanzione edittale, nel termine perentorio di 60 giorni dalla data di notifica della contestazione;
- le fattispecie in cui non è prevista pubblicità dell'irrogazione di sanzioni amministrative.

I **proventi** delle sanzioni amministrative pecuniarie sono versati all'entrata del bilancio dello Stato per essere riassegnati all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale (**comma 16**).

Articolo 39
(Assistenza reciproca)

L'**articolo 39** disciplina le modalità di cooperazione e assistenza reciproca tra l'Autorità nazionale competente NIS e le Autorità competenti degli altri Stati membri.

L'**articolo 39** si basa sulla disposizione dell'**articolo 37** della direttiva (UE) 2022/2055 che disciplina l'assistenza reciproca tra gli Stati membri le cui autorità competenti sono chiamate a cooperare informandosi e chiedendo misure in materia di vigilanza ed esecuzione dell'applicazione della direttiva medesima. Il fine è quello di assistere, proporzionalmente alle proprie risorse, gli Stati membri che necessitino di implementare tali misure.

A norma dell'**articolo 8** della sopracitata direttiva, le autorità competenti NIS-*Network and Information Security* sono i soggetti cui spetta il **controllo dell'applicazione** in quanto responsabili della cybersicurezza e dei compiti di vigilanza. Sono designate da ogni Stato membro il quale può affidare questo ruolo a una o più autorità esistenti. Se uno Stato membro designa o istituisce soltanto un'autorità competente, quest'ultima è anche il **punto di contatto unico** per tale Stato membro.

Lo schema di decreto in commento riconosce all'**articolo 10** l'Agenzia per la cybersicurezza nazionale sia quale "autorità competente", che "punto di contatto unico", nonché quale "*Team* di risposta agli incidenti di sicurezza informatica (CSIRT)".

Si ricorda, in tal proposito, che l'Agenzia per la cybersicurezza nazionale è stata istituita dal decreto legge del 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 legge 4 agosto 2021, n. 109.

Il **comma 1** dell'articolo in commento conferma che l'Autorità nazionale competente NIS, che come detto corrisponde all'Agenzia per la cybersicurezza nazionale, aderisce al circuito di cooperazione e assistenza con le Autorità competenti degli altri Stati membri, e ne regola le modalità di partecipazione.

In particolare, il **comma 1, lettera a)**, dispone che forniscono servizi in uno o più Stati membri i soggetti destinatari della norma ai sensi dell'**articolo 3**, che rientrano anche nella giurisdizione nazionale in quanto, come disciplina invece l'**articolo 5**, sono stabiliti in via principale nel territorio nazionale o in quanto vi sono ubicati i rispettivi sistemi informativi e di rete.

Analogamente, a norma della **lettera b)**, forniscono servizi sul territorio nazionale i soggetti che sono, invece, ritenuti sotto la giurisdizione di altri Stati membri, sempre con riferimento ai criteri di cui all'**articolo 5**, o se vi hanno ubicato i rispettivi sistemi informativi e di rete.

Il **comma 2** precisa che la cooperazione comprende, in particolare, la notifica e la consultazione tramite il Punto di contatto unico NIS (cioè sempre l'Agenzia per la cybersicurezza nazionale, in base all'articolo 10) circa le attività ispettive e le misure di esecuzione (**lettera a)**) che possono essere oggetto di una richiesta giustificata (**lettera b)**) e prevedere interventi di assistenza proporzionata alle risorse per garantire un'attuazione efficace, efficiente e coerente (l**ettera c)**). Tali interventi, ai sensi del **comma 3**, possono riguardare richieste di informazioni e attività ispettive anche in loco o audit sulla sicurezza mirati.

Secondo, l'**articolo 8 della direttiva (UE) 2022/2555** ogni punto di contatto unico svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, e, ove opportuno, con la Commissione e l'Agenzia dell'UE per la sicurezza delle reti e dell'informazione, ENISA, nonché per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro. Come detto, in Italia tale ruolo viene affidato dall'**articolo 10 dello schema di decreto in commento** all'Agenzia per la cybersicurezza nazionale.

Il **comma 4**, contiene disposizioni in merito ai casi in cui l'Autorità nazionale competente NIS possa respingere una richiesta di assistenza. Si tratta, in particolare, dei casi in cui l'Autorità richiedente non è competente (**lettera a)**), oppure se l'attività richiesta non è proporzionata ai compiti previsti dallo schema di decreto (**lettera b)**) o se riguarda attività il cui svolgimento contrasta con gli interessi essenziali di sicurezza nazionale, di pubblica sicurezza o di Difesa dello Stato (**lettera c)**).

A tali fini, il **comma 5** stabilisce che prima di respingere una richiesta l'Autorità nazionale competente consulta le autorità degli Stati membri interessati e su richiesta anche solo di uno di essi può interpellare la Commissione europea e l'ENISA (Agenzia europea per la cybersicurezza).

Ai sensi del **comma 6**, poi, sono previste attività ispettive o di esecuzioni comuni tra le Autorità competenti nazionali.

Il **comma 7** attribuisce, inoltre, alla **lettera a)**, all'Autorità nazionale competente NIS, in caso di richiesta di assistenza da parte di Autorità competenti di altri Stati membri, la possibilità di esercitare i poteri di

monitoraggio, vigilanza ed esecuzione di cui al **Capo V** del presente schema di decreto nei confronti di un soggetto che risponde ai requisiti espressi al **comma 1, lettera a)** dell'articolo in commento.

Infine, secondo la **lettera b) del comma 7**, l'Autorità nazionale competente NIS può anche inoltrare una richiesta di assistenza reciproca alle autorità degli altri Stati membri per l'esercizio dei poteri relativi alle misure di gestione del rischio di cybersicurezza, di cui al **Capo IV della direttiva (UE) 2022/2555**, nei confronti dei soggetti individuati al **comma 1, lettera b)**, dell'articolo in commento.

CAPO VI – DISPOSIZIONI FINALI E TRANSITORIE

Articolo 40
(Attuazione)

L'**articolo 40** disciplina l'adozione dei provvedimenti attuativi previsti dal provvedimento. Si tratta di decreti del Presidente del Consiglio dei ministri (DPCM) e di determinazioni dell'Agenzia per la cybersicurezza nazionale.

Per i DPCM, i **commi 1, 2 e 3** affermano che gli stessi saranno adottati "anche **in deroga** all'articolo 17" della legge n. 400 del 1988, che, come è noto, disciplina l'adozione dei regolamenti da parte del Governo. La deroga sembra essere riferita in particolare a quanto disposto dal comma 1 dell'articolo 17 che prevede infatti che per l'esecuzione, l'attuazione e l'integrazione delle leggi possano essere adottati regolamenti con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri e **sentito il parere del Consiglio di Stato**. In base al comma 4 dell'articolo 17 i regolamenti devono **essere anche registrati dalla Corte dei conti.**

I DPCM oggetto dell'articolo 40 saranno invece adottati su proposta dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS e previo parere del Comitato interministeriale per la cybersicurezza.

I commi da 1 a 3 ricapitolano quelli che sono i DPCM previsti da specifiche disposizioni del provvedimento. Per approfondimenti si rinvia quindi alle relative schede di lettura. Sono richiamati in particolare i DPCM previsti:

- per l'applicazione della clausola di salvaguardia prevista dall'articolo 3, comma 4, e in base alla quale non si applicano i criteri previsti dalla raccomandazione 2003/361/CE per l'individuazione delle medie e grandi imprese rilevanti per il provvedimento se tali criteri non risultano proporzionati (comma 1, lettera a);

In base al successivo **comma 7**, tali DPCM dovranno essere adottati entro trenta giorni dall'entrata in vigore del provvedimento.

- per l'individuazione dei criteri, delle procedure e delle modalità per le attività di vigilanza ai sensi dell'articolo 34, comma 10 (comma 1, lettera b);

In base al successivo **comma 8**, tali DPCM dovranno essere adottati entro sei mesi dall'entrata in vigore del provvedimento.

- per la definizione delle misure di applicazione degli strumenti deflattivi del contenzioso ai sensi dell'articolo 38, comma 15 (comma 1, lettera c);

In base al successivo **comma 8**, tali DPCM dovranno essere adottati entro sei mesi dall'entrata in vigore del provvedimento.

- per l'eventuale individuazione di ulteriori settori ad alta criticità (oltre quelli elencati nell'allegato I del provvedimento), di ulteriori settori critici (oltre quelli elencati nell'allegato II del provvedimento), di ulteriori categorie di soggetti pubblici e privati da ricondurre all'ambito di applicazione del provvedimento oltre quelli individuati ai sensi dell'articolo 3 (comma 2, lettera a);
- di ulteriori categorie di pubbliche amministrazioni da ricondurre al medesimo ambito (comma 2, lettera b);
- per stabilire le modalità di raccordo e di collaborazione tra Agenzia per la cybersicurezza e Autorità di settore NIS di cui all'articolo 11 (cfr. *supra* la relativa scheda di lettura; comma 2, lettera c);

in base al successivo **comma 8**, i DPCM attuativi del comma 2, lettera c), dovranno essere adottati entro sei mesi dall'entrata in vigore del provvedimento.

- per la definizione delle modalità di raccordo tra le diverse amministrazioni ai sensi dell'articolo 14 (comma 3);

in base al successivo **comma 7**, i DPCM attuativi del comma 3 dovranno essere adottati entro trenta giorni dall'entrata in vigore del provvedimento.

Con riferimento ai DPCM attuativi si segnala anche che il **comma 6** esclude dal diritto di accesso e dalla pubblicazione quelli previsti dal comma 3, lettera a). *Al riguardo, si segnala però che il comma 3 non contiene lettere.*

Il **comma 10** prevede infine che i DPCM fin qui richiamati saranno oggetto di aggiornamento periodico e comunque ogni tre anni.

I **commi 4 e 5** ricapitolano quelle che sono le determinazioni che l'Agenzia per la cybersicurezza nazionale dovrà adottare per l'attuazione del provvedimento. Per approfondimenti si rinvia alle schede di lettura degli articoli richiamati.

Per le determinazioni previste dal **comma 4**, l'adozione avverrà su proposta delle autorità di settore NIS interessate, sentito il Tavolo per l'attuazione della disciplina NIS. Si tratta delle determinazioni volte a:

- individuare i concreti soggetti ai quali si applica la clausola di salvaguardia prevista dall'articolo 3, comma 4 e già descritta con riferimento al comma 1, lettera a) (comma 4, lettera a);
- individuare i concreti soggetti ai quali si applicherà il provvedimento ai sensi dell'articolo 3, commi 8 e 9 (sul punto si rinvia alla relativa scheda di lettura; comma 4, lettera b)

In base al successivo **comma 6**, le determinazioni di cui al comma 4, lettera b) saranno escluse dal diritto di accesso e dall'obbligo di pubblicazione. In base al successivo **comma 7,** le medesime determinazioni dovranno essere adottate entro trenta giorni dall'entrata in vigore del provvedimento.

In sostanza quindi, mentre ai DPCM sarà affidata la determinazione di criteri generali o di categorie di soggetti, le determinazioni del comma 4 dovranno in concreto definire i soggetti coinvolti.

Per le determinazioni previste dal **comma 5**, invece, l'adozione avverrà solo sentito il Tavolo per l'attuazione della disciplina NIS. Si tratta delle determinazioni volte a:

- individuare l'elenco dei soggetti essenziali e dei soggetti importanti di cui all'articolo 7, comma 2 (lettera a);

In base al successivo **comma 6**, tali determinazioni saranno escluse dal diritto di accesso e non saranno soggetti a pubblicazione.

- stabilire termini, modalità e procedimenti alla piattaforma digitale destinata ai soggetti che rientrano nell'ambito di applicazione del provvedimento prevista dall'articolo 7, nonché termini, modalità e procedimenti per la designazione del rappresentante nell'UE dei fornitori di servizi di sistema dei nomi di dominio DNS stabiliti fuori dall'UE, ai sensi dell'articolo 5, comma 3 (lettera b);

in base al successivo **comma 7**, tali determinazioni dovranno essere adottate entro trenta giorni dall'entrata in vigore del provvedimento.

- stabilire eventuali ulteriori disposizioni per l'organizzazione e per il funzionamento del Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 (lettera c);

in base al successivo **comma 7**, tali determinazioni dovranno essere adottate entro trenta giorni dall'entrata in vigore del provvedimento.

- adottare, "d'intesa" con il Ministero della giustizia, la politica nazionale di divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 16, comma 4 (lettera d); al riguardo, si ricorda che la Circolare per la formulazione tecnica dei testi legislativi del Presidente della Camera del 20 aprile 2001 prescrive, al paragrafo 4, lettera p), di utilizzare il termine "intesa" per le procedure tra soggetti appartenenti a enti diversi (ad esempio, tra Stato, regioni ed altri enti territoriali) e il termine "concerto" per le procedure tra più soggetti appartenenti allo stesso ente (ad esempio, tra diversi ministri); *si valuti quindi l'opportunità di sostituire il termine "intesa" con il termine "concerto";*

in base al successivo **comma 8**, tali determinazioni dovranno essere adottate entro sei mesi dall'entrata in vigore del provvedimento.

- imporre eventuali condizioni per le informazioni messe a disposizione dalle autorità competenti e dal CSIRT Italia (cioè l'Agenzia per la cybersicurezza nazionale) nel contesto degli accordi di condivisione delle informazioni sulla sicurezza informatica di cui all'articolo 17, comma 3 (lettera e);
- stabilire le modalità con cui i soggetti essenziali e i soggetti importanti notificano la loro partecipazione agli accordi di condivisione delle informazioni sulla sicurezza informatica di cui all'articolo 17, comma 4 (lettera f);

in base al successivo **comma 8**, le determinazioni di cui alla lettera f) dovranno essere adottate entro sei mesi dall'entrata in vigore del provvedimento.

- designare gli esperti di sicurezza informatica di cui all'articolo 21 nonché individuare le modalità di esecuzione della revisione tra pari di cui al medesimo articolo 21 (lettera g);
- imporre l'utilizzo di prodotti, servizi e processi TIC certificati ai sensi dell'articolo 27 (lettera h);

- stabilire le categorie di rilevanza previste dall'articolo 30 (lettera i);

in base al successivo **comma 10**, le determinazioni di cui alla lettera i) dovranno essere adottate entro diciotto mesi dall'entrata in vigore del provvedimento.

- stabilire gli obblighi proporzionati e graduali di cui all'articolo 31 (lettera l);

in base al successivo **comma 8**, tali determinazioni dovranno essere adottate entro sei mesi dall'entrata in vigore del provvedimento.

- stabilire i criteri per la determinazione delle sanzioni ai sensi dell'articolo 38, comma 2.

Il **comma 11** stabilisce infine che le determinazioni dell'Agenzia per la cybersicurezza nazionale previste dall'articolo in commento siano aggiornati periodicamente e, comunque, ogni due anni.

Articolo 41
(Abrogazioni e regime transitorio)

L'**articolo 41** dispone l'abrogazione del d.lgs. n. 65 del 2018 di recepimento della prima direttiva NIS e degli articoli 40 ("Sicurezza delle reti e dei servizi") e 41 ("Attuazione e controllo") del d.lgs. n. 259 del 2003 recante "Codice delle comunicazioni elettroniche", prevedendo una fase transitoria fino all'emanazione dei provvedimenti attuativi del decreto. Si prevede, inoltre, al d.lgs. n. 259 del 2003, l'abrogazione della lettera h) dell'articolo 2, comma 1, e l'abrogazione dell'articolo 30, comma 26.

In particolare, al **comma 1** l'articolo in esame stabilisce che, a decorrere dalla data di entrata in vigore del decreto in esame, il d. lgs. n. 65 del 2018 è abrogato.

Dall'abrogazione sono esclusi l'articolo 7, comma 8 e l'articolo 8, comma 10, del decreto, i quali – recando la copertura degli oneri discendenti, rispettivamente, dall'istituzione e dal funzionamento dell'Autorità nazionale competente NIS e del punto di contatto unico (art. 7) e del CSIRT (art. 8) – sono abrogati dall'anno 2025.

Fino alla data di adozione dei provvedimenti attuativi di cui all'articolo 40, commi 1, 2, 3, 4 e 5, lettere a), b), e) e f), si precisa che nei confronti dei soli soggetti identificati prima della data di entrata in vigore del decreto in esame come operatori di servizi essenziali, i capi IV (Sicurezza della rete e dei sistemi informativi degli operatori di servizi essenziali) e V (Sicurezza della rete e dei sistemi informativi dei fornitori di servizi digitali) del decreto legislativo n. 65 del 2018 continuano a trovare applicazione.

Al **comma 2** si dispone che al codice delle comunicazioni elettroniche (d. lgs. n. 259 del 2003) siano abrogati:

- l'articolo 2, comma 1, la lettera h), recante la definizione di apparecchiature terminali;
- l'articolo 30, comma 26, che introduce sanzioni amministrative pecuniarie per il caso di inosservanza delle disposizioni in materia di sicurezza informatica;
- gli articoli 40 e 41, recanti disposizioni per la sicurezza delle reti e dei servizi.

Al **comma 3** si precisa che i provvedimenti attuativi degli articoli 40 e 41 del codice delle comunicazioni elettroniche continuano a trovare applicazione, per quanto non in contrasto con la legge e con le disposizioni

del decreto in esame, fino all'adozione delle determinazioni di cui all'articolo 40, comma 5, lettera l) chiamate a stabilire l'elenco dei "soggetti essenziali" e dei "soggetti importanti" (per approfondimenti si rinvia alla scheda di lettura dell'articolo 40; per la definizione di "soggetti essenziali" e "soggetti importanti" a quelle degli articoli 6 e 7).

Articolo 42
(Fase di prima applicazione)

L'**articolo 42** regola la **prima fase di applicazione** del presente provvedimento.

Il **comma 1, lett. *a)***, dispone che, in fase di prima applicazione, alcuni dei soggetti essenziali e importanti tenuti alla **registrazione alla piattaforma digitale** ai sensi dell'articolo 7 del presente decreto, sono tenuti a registrarsi entro il **17 gennaio 2025**, si tratta in particolare dei seguenti soggetti:

- i fornitori di servizi di sistema dei nomi di dominio;
- i gestori di registri dei nomi di dominio di primo livello;
- i fornitori di servizi di registrazione dei nomi di dominio;
- i fornitori di servizi di *cloud computing*;
- i fornitori di servizi di data center;
- i fornitori di reti di distribuzione dei contenuti;
- i fornitori di servizi gestiti;
- i fornitori di servizi di sicurezza gestiti;
- i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di *social network.*

Il **comma 1, lett. *b)***, prevede che, fino al 31 dicembre 2025, il **Tavolo per l'attuazione della disciplina NIS** si riunisce almeno una volta ogni 60 giorni (ai sensi dell'art. 12, comma 4, il Tavolo NIS è tenuto, a regine, a riunirsi almeno una volta ogni tre mesi.

Il **comma 1, lett. *c)***, stabilisce che, fino al 31 dicembre 2025, il termine per l'adempimento degli obblighi in materia di **notifica di incidenti** (di cui all'articolo 25) è fissato in 9 mesi dalla ricezione della comunicazione, da parte dell'autorità NIS con la quale viene notificato agli enti interessati l'inserimento nell'elenco dei soggetti essenziali e importanti (si ricorda che le notifiche di incidenti, a regime, devono essere comunicati senza ritardo ai sensi dell'art. 25 alla cui scheda di lettura si rinvia). Parimenti, il termine per l'adempimento degli obblighi di cui agli articoli 23 e 24 (approvazione delle modalità di implementazione delle **misure di gestione dei rischi**) e 29 (realizzazione della **banca dati di registrazione dei nomi di dominio**) è fissato in 18 mesi dalla comunicazione di cui sopra.

Ai sensi del **comma 2** i soggetti essenziali ed importati comunicano l'elenco delle proprie attività a partire dal 1° gennaio 2026 (a regime si prevede che la comunicazione avvenga ogni anno dal 1° maggio al 30 giugno, v. art. 31, comma1).

Infine, i soggetti essenziali e i soggetti importanti possono registrarsi alla **piattaforma digitale** partire dalla data di pubblicazione della medesima piattaforma di cui all'articolo 7, comma 1, cui sono tenuti a registrarsi e ad aggiornare la propria registrazione, a regime. dal 1° gennaio al 28 febbraio di ogni anno (**comma 7**).

Per approfondimenti si rinvia alle schede di lettura degli articoli richiamati.

Articolo 43
(Modifiche normative)

L'**articolo 43** reca alcune modifiche normative ai decreti legge n. 82/2021 e n. 105/2019, volte sia ad assicurare la coerenza delle disposizioni introdotte con l'architettura nazionale di cybersicurezza, con i compiti dell'ACN, nonché con il perimetro di scurezza nazionale cibernetica.

Si ricorda in proposito che tra i criteri di delega previsti dall'articolo 3, co. 1, della legge delegazione europea 2022/2023 si prevede di apportare alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il **coordinamento** con le disposizioni emanate in attuazione dell'articolo in esame (**lettera p**).

In particolare, il **comma 1** reca **modifiche al decreto-legge n. 82/2021** (conv. L. n. 109/2021) che definisce l'architettura nazionale di cybersicurezza e ha istituito l'Agenzia per la cybersicurezza nazionale.

Nel dettaglio, la **lettera *a)*** reca due novelle alle lettere *d)* ed *e)* del comma unico dell'articolo 1 del citato D.L. n. 82/2021, che sostituiscono i riferimenti al decreto legislativo NIS, con cui si farà riferimento solo al provvedimento in esame, in attuazione della direttiva NIS 2, al posto del precedente D.Lgs. n. 65/2018 (attuativo della direttiva NIS).

Con la **lettera *b)*** si apportano analoghe modifiche di aggiornamento dei riferimenti normativi all'articolo 7 del medesimo decreto-legge (lett. *d)*, *d-bis* e *d-ter*), che disciplina le funzioni dell'ACN.
È inoltre abrogato il comma 3 dell'articolo 7, sul trasferimento e cambio di denominazione del «CSIRT Italia». Tale disposizione è infatti superata dalle previsioni contenute all'articolo 15 dello schema in esame (alla cui scheda di lettura, *supra*, si rinvia).

La **lettera *c)*** provvede infine ad **abrogare l'articolo 15 del D.L. n. 82/2021**, con cui è stato novellato il decreto legislativo n. 65 del 2018, di attuazione della direttiva NIS, al fine di adeguarlo alla nuova architettura delineata da quel decreto-legge. Si ricorda infatti che il d.lgs. n. 65/2018 viene sostituito integralmente dallo schema in esame (ed è abrogato dall'articolo 41 del provvedimento).

Con il **comma 2** sono introdotte **modifiche al decreto-legge n. 105 del 2019** (c.d. decreto Perimetro, conv. L. n. 133/2019), che definisce il

perimetro di sicurezza nazionale cibernetica e disciplina i poteri speciali nei settori di rilevanza strategica, al fine, dichiarato dalla stessa disposizione, di assicurare coerenza normativa tra le disposizioni relative agli obblighi in materia di gestione del rischio e notifica di incidente, di cui al Capo IV dello schema in esame, e quelle sulle attività di vigilanza ed esecuzione di cui al Capo VI.

Sul coordinamento con la disciplina del perimetro di sicurezza nazionale cibernetica, si v, anche, *supra*, la scheda di lettura dell'articolo 33.

Nello specifico, tutte le modifiche introdotte dal comma 2 riguardano l'**articolo 1 del D.L. n. 105/2019** e segnatamente:

- è **abrogato il comma 3-*bis*** di tale disposizione, introdotto dall'articolo 37-*quater* del decreto-legge n. 115/2022, che ha esteso gli obblighi di notifica già previsti per gli incidenti aventi impatto su beni destinati a essere impiegati nel Perimetro di sicurezza nazionale cibernetica (beni ICT), anche agli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (diversi quindi dai beni ICT), ma che sono di pertinenza di soggetti inclusi nel Perimetro (**lettera *a)***);

- è sostituito il **comma 8**, che determina alcuni obblighi di sicurezza e di notifica di incidente per: gli operatori dei servizi essenziali; i fornitori di servizi digitali; le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, inclusi nel perimetro di sicurezza nazionale cibernetica. In luogo della attuale disposizione si prevede, da un lato, che la notifica di incidente ai sensi del comma 3, lettera a), effettuata dai **soggetti inclusi nel perimetro** di sicurezza nazionale cibernetica **che rientrano nell'ambito di applicazione del decreto legislativo di recepimento della direttiva NIS 2** assolve agli obblighi in materia di notifica di incidente di cui all'articolo 25 del medesimo d.lgs. (**lettera *b)***)

- è introdotto un **comma 8-bis** il quale estende ai **soggetti inclusi nel perimetro** che **non sono individuati come soggetti essenziali o importanti** ai sensi degli articoli 3 e 6 del decreto in esame, gli obblighi di cui al capo IV e le attività ispettive e sanzionatorie di cui al capo V per i soggetti essenziali ai sensi del medesimo decreto, limitatamente ai sistemi informativi e di rete diversi da quelli inseriti nell'elenco delle reti, dei sistemi informativi e dei servizi informatici. Tale disposizione dovrà essere gradualmente implementata sulla base di modalità e termini stabiliti dall'ACN con propria determina, sentito il tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale (**lettera *c)***);

- è **abrogato il comma 17** dell'articolo 1 sul Perimetro, che reca due novelle al decreto legislativo n. 65 del 2018 (di attuazione della direttiva NIS), sostituito dal provvedimento in esame (**lettera *d)***).

Articolo 44
(Disposizioni finanziarie)

L'**articolo 44** reca le disposizioni finanziarie. In particolare, il **comma 1** afferma la **coerenza delle spese ICT** *(Information and Communications Technology)* **sostenute dalle pubbliche amministrazioni** in base alle disposizioni del presente decreto e, più in generale, delle spese ICT sostenute **per l'adeguamento dei sistemi informativi** a quanto previsto dal **Piano triennale per l'informatica nella pubblica amministrazione**.
Il **comma 2** reca la norma di **copertura finanziaria degli oneri** determinati dalle spese ICT autorizzate dal decreto in esame. Il **comma 3** prevede le ulteriori **disposizioni finanziarie**.

In particolare, il **comma 1** è volto ad affermare la coerenza delle **spese ICT** *(Information and Communications Technology)* **sostenute dalle pubbliche amministrazioni** ai sensi delle disposizioni del **presente decreto**, nonché, più in generale, delle spese ICT sostenute **per l'adeguamento dei sistemi informativi** a quanto previsto dal **Piano triennale per l'informatica nella pubblica amministrazione**.

Il **Piano triennale** per l'informatica nella pubblica amministrazione, introdotto con la legge n. 208 del 2015 (art. 1, commi dal 512 a 520), ha rappresentato lo strumento principale per la **pianificazione** delle azioni di **digitalizzazione della P.A.**, attraverso la declinazione della strategia in materia di digitalizzazione in indicazioni operative, quali obiettivi e risultati attesi, riconducibili all'azione amministrativa delle PA. Il **Piano 2024-2026,** approvato con il D.P.C.M.12 gennaio 2024, si inserisce nel più ampio contesto di riferimento definito dal programma strategico "Decennio Digitale 2030", istituito dalla Decisione (UE) 2022/2481 del Parlamento Europeo e del Consiglio del 14 dicembre 2022, i cui obiettivi sono articolati in quattro dimensioni: competenze digitali, servizi pubblici digitali, digitalizzazione delle imprese e infrastrutture digitali sicure e sostenibili. Per la prima volta, il Piano affronta anche il tema **dell'Intelligenza Artificiale**, fornendo indicazioni e principi generali che dovranno essere adottati dalle amministrazioni e declinati in fase di applicazione, tenendo in considerazione lo scenario in rapida evoluzione.

Il **comma 2** concerne la **copertura finanziaria** degli **oneri**, quantificati complessivamente in **409.424 euro** per l'anno **2024** e **5.925.695 euro annui a** decorrere **dall'anno 2025**, derivanti dalle seguenti disposizioni:

- articolo 10 (individuazione **dell'Autorità nazionale competente NIS** e del Punto di contatto unico NIS),
- articolo 11 (individuazione delle **Autorità di settore NIS**),

- articolo 13, comma 1 (individuazione delle **Autorità nazionali di gestione delle crisi informatiche**),
- articolo 15 (costituzione del Gruppo nazionale di risposta agli incidenti di sicurezza informatica – **CSIRT Italia**).

A tali oneri si provvede:

a) quanto a 409.424 euro per l'anno 2024, 2.625.695 euro per l'anno 2025, 2.707.695 euro per l'anno 2026 e 3.100.695 euro annui a decorrere dall'anno 2027, mediante corrispondente **riduzione del Fondo per il recepimento della normativa europea**

   Si tratta del Fondo istituito dall'41-*bis* della legge n. 234 del 2012, Al fine di consentire il tempestivo adeguamento dell'ordinamento interno agli obblighi imposti dalla normativa europea, nei limiti occorrenti per l'adempimento degli obblighi medesimi qualora non sia possibile farvi fronte con i fondi già assegnati alle competenti amministrazioni;

b) quanto a 3.300.000 euro per l'anno 2025, 3.218.000 euro per l'anno 2026 e 2.825.000 euro annui a decorrere dall'anno 2027, mediante **utilizzo delle risorse** rivenienti **dall'abrogazione** di alcune delle disposizioni del **D.Lgs. n. 65 del 2018**, di attuazione della direttiva (UE) 2016/1148 (prima direttiva NIS), disposta dall'articolo 41, comma 1, del presente provvedimento (*si rinvia alla relativa scheda*).

Il **comma 3** contiene la **clausola di invarianza finanziaria** riferita all'attuazione delle restanti disposizioni dello schema di decreto in esame, dalle quali non devono derivare effetti finanziari negativi a carico della finanza pubblica.

Allegato

La disciplina della sicurezza cibernetica

La direttiva NIS 1

La materia della sicurezza cibernetica è regolata a livello dell'Unione europea dalla direttiva (UE) 2016/1148 del 6 luglio 2016 (c.d. **direttiva NIS** - *Network and Information Security*) che reca misure per conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea. La direttiva è stata recepita nell'ordinamento interno con il **decreto legislativo n. 65 del 18 maggio 2018**, che costituisce la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS.

La normativa europea è stata aggiornata dalla direttiva (UE) 2022/2555 del 14 dicembre 2022 (c.d. **direttiva NIS 2**) - oggetto del provvedimento in esame - al fine di tener conto di una crescente digitalizzazione del mercato interno e di un panorama in evoluzione delle minacce alla cibersicurezza. L'aggiornamento della direttiva mira inoltre ad eliminare le ampie divergenze tra gli Stati membri che hanno attuato gli obblighi in materia di sicurezza e segnalazione degli incidenti, nonché in materia di vigilanza ed esecuzione, stabiliti dalla direttiva NIS in modi significativamente diversi a livello nazionale, con un effetto potenzialmente pregiudizievole sul funzionamento del mercato interno. La delega per la trasposizione della direttiva nel diritto interno è contenuta nella **legge di delegazione europea 2022-2023** (L. 15/2024).

Il perimetro della sicurezza nazionale cibernetica

Successivamente alla attuazione della NIS 1, il **decreto-legge n. 105 del 2019** è stato adottato al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle **amministrazioni pubbliche**, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un **perimetro di sicurezza nazionale cibernetica (PNSC)** e la previsione di misure volte a garantire i necessari *standard* di sicurezza rivolti a minimizzare i rischi. Talune modifiche sono state apportate, a tale provvedimento, dal decreto-legge n. 162 del 2019.

La governance del sistema di sicurezza cibernetica

Con il **decreto-legge n. 82 del 2021**, si è proceduto alla definizione dell'**architettura nazionale di cybersicurezza** e all'istituzione dell'**Agenzia per la cybersicurezza nazionale**, in attuazione di precisi obiettivi del Piano nazionale di ripresa e resilienza (**PNRR**): la sicurezza cibernetica costituisce, infatti, uno dei principali interventi previsti dal PNRR nell'ambito della trasformazione digitale della p.a. e della digitalizzazione del Paese (vedi oltre).

La *governance* del sistema di sicurezza cibernetica ha al suo vertice il **Presidente del Consiglio dei ministri**, al quale è attribuita l'alta direzione e la responsabilità generale delle politiche di cybersicurezza nonché l'adozione della relativa strategia nazionale e - previa deliberazione del Consiglio dei ministri - la nomina e la revoca dei vertici dell'Agenzia per la cybersicurezza nazionale; i tali nomine sono preventivamente informati il COPASIR e le competenti Commissioni parlamentari. Il Presidente del Consiglio dei ministri può delegare all'**Autorità delegata per il sistema di informazione per la sicurezza della Repubblica**, ove istituita, le funzioni in materia di sicurezza cibernetica che non sono a lui attribuite in via esclusiva.

Presso la Presidenza del Consiglio dei ministri è istituito il **Comitato interministeriale per la cybersicurezza (CIC)**, organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

L'**Agenzia per la cybersicurezza nazionale (ACN)** è istituita a tutela degli interessi nazionali nel campo della cibersicurezza. L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. L'Agenzia è l'Autorità nazionale per la cybersicurezza e in quanto tale ha il coordinamento tra i soggetti pubblici coinvolti nella cibersicurezza a livello nazionale; promuove azioni comuni dirette ad assicurare la sicurezza cibernetica, a sviluppare la digitalizzazione del sistema produttivo e delle pubbliche amministrazioni e del Paese, nonché a conseguire autonomia (nazionale ed europea) per i prodotti e processi informatici di rilevanza strategica, a tutela degli interessi nazionali nel settore. Essa predispone la **strategia nazionale di cibersicurezza**. Ai sensi del nuovo Codice europeo delle comunicazioni elettroniche, svolge anche i compiti relativi alla sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico e alla protezione dalle minacce informatiche delle comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone altresì la resilienza (D.Lgs. 8 novembre 2021, n. 207, art. 6, comma 3 e artt. 40 e 41). Presso l'Agenzia per la cybersicurezza nazionale è prevista la costituzione di un **Nucleo per la cybersicurezza**, per profili attinenti a eventuali situazioni di crisi.

Il Presidente del Consiglio dei ministri trasmette al Parlamento (entro il 30 aprile di ogni anno) una **relazione** sull'attività svolta dall'Agenzia nell'anno precedente. Così come trasmette al COPASIR (entro il 30 giugno di ogni anno) una relazione sulle attività svolte nell'anno precedente dall'Agenzia concernenti la tutela della sicurezza nazionale nello spazio cibernetico per i profili di competenza del Comitato.

Le risorse del PNRR per la cibersicurezza

Nell'ambito del **PNRR** la Cybersecurity è uno dei 7 investimenti afferenti alla Digitalizzazione della pubblica amministrazione, primo asse di intervento della componente 1 "Digitalizzazione, innovazione e sicurezza nella PA" compresa nella Missione 1 "Digitalizzazione, innovazione, competitività, cultura e turismo".

L'investimento (**investimento 1.5**) è volto alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese a partire dalla attuazione della disciplina prevista dal perimetro di sicurezza nazionale cibernetica; ad esso sono destinati 622 milioni di euro di cui:

- 241 per la creazione di una infrastruttura per la cybersicurezza (attuata con la creazione della ACN);
- 231 per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica PNSC;
- 150 per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'Interno, ministero della Difesa, Guardia di Finanza, ministero della Giustizia e Consiglio di Stato.

L'intervento si articola in 4 aree principali:

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

L'investimento è finalizzato a garantire il funzionamento dell'intero sistema di digitalizzazione della p.a. che prevede in primo luogo la creazione di infrastrutture digitali per la p.a. anche attraverso la realizzazione del Polo strategico nazionale (investimento 1.1). Si tratta di un ambiente *cloud* destinato ad ospitare la Piattaforma digitale nazionale dati ove confluiranno le informazioni provenienti da tutte le amministrazioni, consentendo

l'interoperabilità dei dati (investimento 1.3). L'obiettivo finale è di sviluppare, attraverso la piattaforma, un'offerta integrata e armonizzata di servizi digitali per i cittadini (investimento 1.4). In tutte queste fasi è necessario garantire la sicurezza cibernetica delle infrastrutture e dei dati.

Il traguardo intermedio previsto dal PNRR, del dicembre 2022, è stato raggiunto con la istituzione dell'Agenzia per la cibersicurezza nazionale – ACN e con il dispiego iniziale dei servizi nazionali di cibersicurezza.

L'obiettivo finale è previsto nel dicembre 2024 con il dispiego integrale dei servizi nazionali di cibersicurezza, l'attivazione delle squadre di pronto intervento informatico (CERT); la piena operatività dei servizi di gestione dei rischi di cibersicurezza, compresi quelli per l'analisi della catena di approvvigionamento e i servizi di assicurazione contro i rischi informatici; il completamento della rete di laboratori e dei centri per la valutazione e certificazione della cibersicurezza; la piena operatività dell'unità centrale di audit.

Reati informatici e cybersicurezza

Il 2 luglio 2024 è stata pubblicata nella *Gazzetta Ufficiale* la **legge 28 giugno 2024, n. 90**, originata da un disegno di legge di iniziativa governativa, in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

Il provvedimento si articola in due parti.

Il Capo I del disegno di legge, reca disposizioni concernenti la cybersicurezza nazionale finalizzate a conseguire una più elevata capacità di protezione e risposta di fronte a emergenze cibernetiche.

Un primo gruppo di disposizioni riguardano le misure da adottare in caso di incidenti informatici.

In particolare viene introdotto un obbligo di segnalazione di alcune tipologie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici in carico alle pubbliche amministrazioni. Nel contempo, le pubbliche amministrazioni qualora siano oggetto di segnalazioni dell'Agenzia per la cybersicurezza nazionale circa specifiche vulnerabilità cui essi risultano potenzialmente esposti, debbano provvedere tempestivamente all'adozione degli interventi risolutivi indicati dalla stessa Agenzia. Si stabilisce che i soggetti inclusi nel Perimetro provvedono, oltre che alla notifica, anche alla segnalazione degli incidenti che intervengono su reti, sistemi informativi e servizi informatici che si trovano al di fuori del Perimetro (di loro pertinenza), senza ritardo e comunque al massimo entro ventiquattro ore e si prevede che i dati relativi a incidenti informatici sono

raccolti, sulla base degli adempimenti di notifica previsti a legislazione vigente, dall'Agenzia per la cybersicurezza nazionale.

Un secondo gruppo di disposizioni interviene sull'architettura della sicurezza cibernetica e sui rapporti tra i diversi attori del sistema, prevedendo:

- la possibilità di far partecipare alle riunioni del Nucleo per la cybersicurezza ulteriori soggetti quali rappresentanti della Direzione nazionale antimafia e antiterrorismo e rappresentanti della Banca d'Italia, in relazione a specifiche questioni di particolare rilevanza concernenti i compiti di proposta di iniziative in materia di cybersicurezza del Paese;
- il potere del Presidente del Consiglio di disporre il differimento degli obblighi informativi e delle attività di resilienza in capo all'Agenzia per la cybersicurezza nazionale nei casi in cui questo sia considerato strettamente necessario dai servizi di sicurezza della Repubblica;
- la modifica la composizione del Comitato interministeriale per la sicurezza della Repubblica (CISR), disponendo che del Comitato facciano parte anche il Ministro dell'agricoltura, il Ministro delle infrastrutture e dei trasporti e il Ministro dell'università e della ricerca;
- l'istituzione per le pubbliche amministrazioni, dove non sia già presente, della struttura preposta alle attività di cyber-sicurezza e del referente per la cyber-sicurezza

Inoltre, vengono rafforzate le misure di sicurezza dei dati attraverso l'uso della crittografia: viene istituito il Centro nazionale di crittografia presso l'Agenzia per la cybersicurezza nazionale e si attribuisce alle strutture preposte alle attività di cybersicurezza nelle pubbliche amministrazioni la funzione di verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica rispettino le linee guida sulla crittografia adottate dall'Agenzia per la cybersicurezza nazionale e dall'Autorità garante per la protezione dei dati personali.

Il provvedimento reca alcune altre disposizioni relative all'Agenzia per la cybersicurezza nazionale:

- sono definiti termini e modalità per l'adozione del regolamento che stabilisce i criteri, anche temporali, per l'accertamento, la contestazione e la notificazione delle violazioni della normativa in materia di cybersicurezza e l'irrogazione delle relative sanzioni di competenza dell'Agenzia;
- si stabilisce un divieto, della durata di due anni, di assunzione, anche di incarichi, presso soggetti privati finalizzata allo svolgimento di mansioni in materia di cybersicurezza per i dipendenti appartenenti al ruolo del personale dell'Agenzia per la cybersicurezza nazionale - ACN che abbiano

partecipato, nell'interesse e a spese dell'Agenzia stessa, a specifici percorsi formativi di specializzazione.

Il disegno di legge introduce alcuni criteri di cybersicurezza nella disciplina dei contratti pubblici e individua nuovi principi e criteri direttivi specifici a cui il Governo dovrà attenersi nel recepimento della normativa europea in materia di resilienza operativa digitale per il settore finanziario.

Infine, vengono introdotte alcune cause di incompatibilità per il personale degli organismi di informazione per la sicurezza (DIS, AISE e AISI) per i tre anni successivi alla cessazione dell'incarico i alla cessazione del servizio.

Il Capo II del provvedimento reca disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari.

In particolare, vengono apportate numerose modifiche al codice penale volte a rafforzare le previsioni in materia di prevenzione e contrasto dei reati informatici, da un lato, prevedendo inasprimenti di pene o ulteriori circostanze aggravanti rispetto alle fattispecie di reati informatici previste a legislazione vigente e, dall'altro, introducendo nuove fattispecie delittuose quali, ad esempio, l'estorsione mediante reati informatici di cui al novellato articolo 629 c.p.. Allo stesso tempo, al fine di rafforzare gli strumenti di contrasto dei reati informatici, viene prevista l'estensione del termine ordinario di conclusione delle indagini preliminari qualora i reati informatici siano commessi in danno di sistemi informatici o telematici di interesse militare o comunque di interesse pubblico.

Inoltre, il provvedimento prevede l'estensione dell'applicazione della speciale disciplina delle intercettazioni prevista per i fatti di criminalità organizzata ai reati informatici rimessi al coordinamento del procuratore nazionale antimafia e antiterrorismo (ovvero i reati di accesso abusivo a sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche; falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o

comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici di pubblica utilità).

Si prevede altresì il rafforzamento della collaborazione tra l'Agenzia per la cybersicurezza nazionale (ACN), il procuratore nazionale antimafia e antiterrorismo, la polizia giudiziaria ed il pubblico ministero, prevedendo, tra l'altro, l'introduzione dell'obbligo di immediata trasmissione delle notizie dei gravi delitti informatici, al fine di procedere ad una tempestiva azione di contrasto degli stessi.

Su altro fronte, viene estesa agli autori dei reati informatici la disciplina di cui al decreto-legge n. 8 del 1991, relativa alla concessione delle speciali misure di protezione e dei benefici penitenziari che possono essere riservati ai soggetti che collaborano con la giustizia.

Infine, si segnala che è stata introdotta la previsione ai sensi della quale l'ispettorato generale presso il Ministero della giustizia, nell'ambito delle ispezioni ordinarie condotte presso gli uffici giudiziari, è chiamato a verificare il rispetto delle prescrizioni di sicurezza negli accessi alle banche dati in uso.