RELAZIONE ILLUSTRATIVA

Il presente decreto legislativo, di recepimento della 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 NIS2)" – che, conseguentemente, abroga a sua volta il d.lgs. 18 maggio 2018, n. 65, di recepimento della direttiva (UE) 2016/1148 (direttiva NIS) – si suddivide in 6 Capi e 44 articoli, riproponendo la struttura della direttiva NIS2 alla luce dei principi e dei criteri introdotti dall'articolo 3 della legge 21 febbraio 2024, n. 15 (legge di delegazione europea 2022-2023).

Si segnala preliminarmente che, nel corso della redazione del presente schema di decreto legislativo, si è optato per una redistribuzione dei contenuti della direttiva NIS2 volta a favorire maggiore organicità al testo del provvedimento, in linea con i principi e i criteri previsti dalla legge di delegazione europea 2022-2023 e con l'attuale impianto della direttiva NIS, come recepito con il richiamato d.lgs. n. 65 del 2018. Ne consegue che, all'esito della razionalizzazione dell'impianto normativo, a fronte dei 9 Capi contenuti nella direttiva NIS2, il presente decreto è strutturato nei seguenti 6 Capi:

- il **Capo I** dedicato alle disposizioni generali che, al suo articolo 5, recepisce anche il Capo V (Giurisdizione e registrazione) della direttiva NIS2;
- il **Capo II** dedicato al quadro nazionale di sicurezza informatica che, al suo articolo 17, recepisce anche il Capo VI (Condivisione delle informazioni) della direttiva NIS2;
- il **Capo III** dedicato alla cooperazione a livello dell'Unione europea e internazionale che, al suo articolo 18 (Gruppo di cooperazione NIS), recepisce anche parte dei due articoli che compongono il Capo VIII (Atti delegati e atti di esecuzione) della direttiva NIS2;
- il **Capo IV** dedicato agli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente che, al suo articolo 27 (Uso di schemi di certificazione della cybersicurezza), recepisce parte dei due articoli che compongono il Capo VIII (Atti delegati e atti di esecuzione) della direttiva NIS2;
- il **Capo V** dedicato alla supervisione che recepisce e razionalizza le disposizioni contenute al Capo VII (Vigilanza ed esecuzione) della direttiva NIS2;
- il **Capo VI** dedicato alle disposizioni finali e transitorie che recepisce il Capo IX (Disposizioni Finali) della direttiva NIS2.

Si evidenzia poi che il dettato normativo, ai fini di assicurare la massima coerenza possibile nell'ordinamento giuridico ed evitare aporie interpretative, è stato elaborato integrando riferimenti legislativi e definizioni già recati dalla disciplina nazionale in materia di cybersicurezza. In particolare, l'articolo 2 amplia in modo mirato il catalogo delle definizioni recate dall'articolo 6 della direttiva al fine di favorire la coerenza con l'impianto normativo nazionale nella materia della cybersicurezza. Con riferimento, poi, alle integrazioni alla disciplina della direttiva NIS2 apportate dall'articolo 3, si segnala, al comma 4, l'introduzione della facoltà di deroga alla disciplina dettata per i gruppi di imprese di cui alla raccomandazione 2003/361/CE – in linea con il considerando 16 della direttiva NIS2 – al fine di promuovere un'attuazione proporzionata e, al comma 6, l'estensione dell'ambito di applicazione della nuova disciplina, introdotta dal presente decreto, alle pubbliche amministrazioni, anche indipendentemente dalle loro dimensioni, con un espresso rinvio, per la categorizzazione, all'allegato III del presente decreto. Tale distinzione in categorie di amministrazioni è necessaria, in particolare, al fine di distinguere quelle ritenute soggetti essenziali da quelle ritenute soggetti importanti.

L'impostazione seguita nell'elaborazione del presente decreto è in linea con quanto previsto dal disegno di legge recante ªDisposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informaticiº (c.d. ddl ªCybersicurezzaº), che per primo ha introdotto alcuni obblighi ± tra i quali l'obbligo di notifica di incidente ± in capo alle pubbliche amministrazioni centrali, alle regioni, alle province autonome di Trento e di Bolzano, alle città metropolitane, ai comuni con popolazione superiore a 100.000 abitanti e, comunque, ai comuni capoluoghi di regione, nonché alle società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, alle società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane e alle aziende sanitarie locali, adottando un regime sanzionatorio che, ai fini dell'armonizzazione normativa richiesta dalla legge di delegazione europea 2022-2023, è stato riproposto nel presente decreto. In un'ottica di omogeneità del sistema sanzionatorio in materia di cybersicurezza, è stata esercitata la facoltà, attribuita dalla direttiva NIS2 a ciascuno Stato membro, di irrogare sanzioni anche nei confronti delle pubbliche amministrazioni. Ai sensi della legge di delegazione europea 2022-2023, è stato anche inserito il riferimento ai soggetti considerati critici ai fini delle attività di interesse culturale e agli istituti di istruzione che svolgono attività di ricerca, così come, in linea con quanto previsto dal ddl Cybersicurezza, è stata estesa l'applicazione della nuova normativa anche ad alcuni soggetti del trasporto pubblico locale e alle società in house, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, che vengono separatamente elencate nell'allegato IV (Altre tipologie di soggetti) di nuova introduzione. Le parti dell'articolo 2 della direttiva NIS2, che attengono a norme o procedure di competenza degli organismi europei, sono state inserite limitatamente agli obblighi in capo ai soggetti attuatori a livello nazionale, ad eccezione di quelli che ne discendono in materia di comunicazioni all'UE, che sono stati trattati all'articolo 22 del presente decreto.

Ciò premesso, più nel dettaglio, il **Capo I** è dedicato alle disposizioni generali per l'attuazione di un livello elevato di sicurezza cibernetica.

L'**articolo 1** definisce l'oggetto del presente decreto legislativo confermando, al comma 2, lettera c), l'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS, Punto di contatto unico NIS e Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente (CSIRT Italia) in ambito nazionale e, tra l'altro:

- designando, al comma 2, lettera d), l'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore, ai sensi dell'articolo 9, paragrafo 2, della direttiva NIS2, ed il Ministero della difesa, ciascuno per gli ambiti di competenza indicati all'articolo 2, comma 1, lettera g), dello schema di decreto, quali autorità competenti alla gestione degli incidenti e delle crisi su vasta scala di cui all'articolo 9 della direttiva NIS2, e cioè quali Autorità nazionali di gestione delle crisi informatiche (ferme restando le competenze del Nucleo per la Cybersicurezza di cui all'articolo 9 del decreto-legge 14 giugno 2021, n. 82);
- prevedendo, al comma 2, lettera e), l'individuazione delle Autorità di settore NIS;
- prevedendo, al comma 2, lettera f), l'indicazione dei criteri per l'individuazione dei soggetti a cui si applica il presente decreto e la definizione dei relativi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente.

Tale impostazione riprende quanto già sancito dal decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, che, nell'attribuire all'Agenzia la funzione di Autorità nazionale di cybersicurezza, ha istituito presso quest'ultima, in via permanente, il Nucleo per la cybersicurezza, a supporto del Presidente del Consiglio dei ministri per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi cibernetiche e per l'attivazione delle procedure di allerta.

L'**articolo 2** contiene le definizioni più ricorrenti nel testo del presente decreto, di cui alcune, ancora attuali, sono mutuate dall'abrogando d.lgs. n. 65 del 2018, mentre altre sono di diretta derivazione unionale. Giova tuttavia segnalare che, al fine di evitare ambiguità interpretative, nel definire la «sicurezza dei sistemi informativi e di rete», non sono stati impiegati i termini «cybersicurezza» o «cibersicurezza» ± quest'ultimo presente nella direttiva NIS2 ±, in quanto tali definizioni sono già contenute in altre fonti normative con accezioni differenti. In particolare, l'articolo 1, comma 1, lettera a), del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, ricomprende, nella definizione di «cybersicurezza», anche le finalità di «tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico», espressamente escluse dalla direttiva NIS2. È stata quindi adottata la definizione «sicurezza informatica», che meglio si adatta agli obiettivi e alle finalità del presente decreto, evitando sovrapposizioni normative. Con riferimento, infine, alle «Autorità nazionali di gestione delle crisi informatiche», di cui si è già fatto cenno nell'ambito dell'illustrazione dell'articolo 1, comma 2, lettera d), viene specificato che il Ministero della difesa svolga la propria funzione di Autorità nazionale di gestione delle crisi informatiche per la parte relativa alla difesa dello Stato e che l'Agenzia per la cybersicurezza nazionale svolga la funzione di Autorità nazionale di gestione delle crisi informatiche per la parte relativa alla resilienza nazionale di cui all'articolo 1 del decreto-legge n. 82 del 2021, assumendo altresì, ai sensi dell'articolo 9, paragrafo 2, della direttiva NIS2, la funzione di coordinatore (richiesta dalla stessa direttiva proprio nell'ipotesi in cui gli Stati membri individuino più di un'autorità nazionale di gestione delle predette crisi su vasta scala).

L'**articolo 3** definisce l'ambito di applicazione dello stesso schema di decreto legislativo, 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. Tale disposizione, al fine di superare l'attuale disomogeneità nel processo di identificazione dei soggetti da parte degli Stati membri, introduce (ai commi 2, 3 e 4) il criterio di individuazione dei soggetti su base dimensionale (corrispondente alla c.d. «*size-cap rule*»), estendendo, rispetto al sistema delineato dalla direttiva NIS, l'applicazione della direttiva NIS2 a tutte le medie e grandi imprese che operano nei settori di cui agli allegati I e II. Sono altresì inclusi nell'ambito applicativo del presente schema di decreto (comma 5), indipendentemente dalla loro dimensione, i soggetti, identificati come «soggetti critici», ai quali si applica la direttiva CER; i fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico, i prestatori di servizi fiduciari, i gestori di registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio, nonché i fornitori di servizi di registrazione dei nomi di dominio. Il comma 6 estende l'ambito di applicazione della nuova disciplina alle pubbliche amministrazioni di cui all'allegato III; il comma 8 individua, anche ai sensi dell'articolo 3 della legge di delegazione europea 2022-2023, i soggetti elencati nell'allegato IV come nuovi soggetti NIS2 indipendentemente dalle loro dimensioni. Il comma 9 prevede espressamente l'applicazione delle nuove norme ai soggetti delle tipologie di cui agli allegati I, II e IV, indipendentemente dalle loro dimensioni, laddove soddisfino determinati requisiti. Il comma 14 prevede che non si applicano ai soggetti identificati come essenziali o importanti dei settori 3 e 4 di cui all'allegato I le disposizioni di cui all'articolo 17 e ai Capi IV e V del presente decreto, ai quali si applica la disciplina di cui al regolamento (UE) 2022/2554. Il comma 15, infine, dispone che il presente decreto non si applica, ai sensi dell'articolo 2, comma 10, della direttiva, ai soggetti esentati dall'ambito di applicazione del regolamento (UE) 2022/2554.

L'**articolo 4** reca disposizioni in materia di protezione degli interessi nazionali e commerciali, chiarendo che rimane impregiudicata ± ai sensi di quanto sancisce l'articolo 4, paragrafo 2, del

Trattato sull'Unione europea ± la responsabilità dello Stato italiano di tutelare la propria sicurezza nazionale e il suo potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale e il mantenimento dell©ordine pubblico.

In ossequio al criterio di ricollocazione sistematica sopra indicato, all'articolo 4 del presente decreto sono state fatte confluire le disposizioni di cui all'articolo 2, commi 6, 7, 8, 9, 11 e 13, della direttiva NIS2, in quanto afferenti alla protezione degli interessi nazionali e commerciali.

Rileva la previsione del comma 4, il quale prevede che con uno o più decreti del Presidente del Consiglio dei ministri, adottati anche su proposta dei Ministri della giustizia, dell'interno e della difesa, per gli ambiti di rispettiva competenza, d'intesa con l'Agenzia per la cybersicurezza nazionale, sono individuati i soggetti che svolgono attività o forniscono servizi in via esclusiva per gli enti, organi e articolazioni della pubblica amministrazione di cui al comma 3 (e cioè quelle che operano nei settori della pubblica sicurezza, della difesa nazionale, o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati, nonché gli organismi di informazione per la sicurezza, di cui agli articoli 4, 5 e 6 della legge n. 124 del 2007, e l'Agenzia per la cybersicurezza nazionale), nonché in materia di protezione civile.

Il comma 5, poi, dispone che, con decreto del Presidente del Consiglio dei ministri, adottato ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, sono individuati i soggetti che svolgono attività o forniscono servizi in via esclusiva per i medesimi organismi di informazione per la sicurezza nazionale.

L'**articolo 5** detta le regole in materia di giurisdizione e territorialità per l'applicazione del presente decreto legislativo, con particolare riferimento ai soggetti transfrontalieri.

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

L'**articolo 7** disciplina le modalità di identificazione dei soggetti essenziali, importanti e che erogano servizi transfrontalieri, tramite registrazione sulla piattaforma digitale, resa disponibile dall'Agenzia per la cybersicurezza nazionale, in linea con quanto previsto all'ultimo capoverso del paragrafo 4 dell'articolo 3 della direttiva NIS2 (ª*Gli Stati membri possono istituire meccanismi nazionali che consentano alle entità di registrarsi.*°). La fascia temporale prevista dal primo comma (ª*Dal 1° gennaio al 28 febbraio di ogni anno successivo all'entrata in vigore del presente decreto*º) per la registrazione dei soggetti o l'aggiornamento dei dati inseriti in piattaforma al momento della registrazione, è funzionale all'aggiornamento periodico dell'elenco dei soggetti essenziali e importanti trasmesso alla Commissione, prescritto, ai sensi dell'articolo 3, paragrafo 3, della direttiva NIS2, con una frequenza almeno biennale. La cadenza annuale appare coerente, da una parte, con i citati parametri della stessa direttiva (cadenza almeno biennale) e appare anche funzionale ad assicurare una attuazione lineare del presente decreto, mitigando gli effetti di isteresi che variazioni repentine, ma limitate nel tempo, del numero di dipendenti dei soggetti possono determinare.

L'**articolo 8** detta, quindi, disposizioni in materia di protezione dei dati personali e di coordinamento con i poteri sanzionatori del Garante per la protezione dei dati personali, richiamando, in particolare, l'applicazione della disciplina di cui al decreto legislativo 30 giugno 2003, n. 196, e del regolamento (UE) 2016/679 (GDPR).

Il **Capo II** è dedicato al quadro nazionale di sicurezza cibernetica.

L'**articolo 9** reca disposizioni in materia di strategia nazionale di cybersicurezza, aggiornando, sulla base delle disposizioni della direttiva NIS2, quanto già previsto dall'abrogando d.lgs. n. 65 del 2018. Viene quindi confermato il vigente impianto che prevede la disciplina del sistema di *governance* della strategia affidata al decreto-legge n. 82 del 2021 ± che definisce, tra l'altro,

l'architettura nazionale di cybersicurezza ± e la definizione dei contenuti della strategia nella disciplina di recepimento della direttiva NIS (e, ora, pertanto, della direttiva NIS2).

Gli **articoli 10** e **11** confermano ± anche in attuazione dell'articolo 3, comma 1, lettera d), della legge di delegazione europea 2022-2023, che prevede di ª *confermare la distinzione tra l@Agenzia per la cybersicurezza nazionale, quale autorità nazionale competente e punto di contatto, ai sensi dell@articolo 8 della direttiva (UE) 2022/2555, e le autorità di settore operanti negli ambiti di cui agli allegati I e II alla medesima direttiva;*º ± da un lato, l'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS e punto di contatto unico NIS e, dall'altro, i Ministeri, già competenti ai sensi dell'abrogando d.lgs. n. 65 del 2018, quali Autorità di settore per l'attuazione della direttiva NIS2. È infine previsto che le Autorità di settore, per taluni ambiti, si coordinino con le Regioni interessate secondo modalità che verranno stabilite tramite un apposito accordo che andrà definito, entro il 30 settembre 2024, in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano.

Ciascuna autorità di settore è autorizzata a reclutare, n. 2 unità di personale non dirigenziale, appartenente all'area funzionari del vigente contratto collettivo nazionale - Comparto funzioni centrali, o categorie equivalenti.

L'**articolo 12** istituisce, in via permanente, il Tavolo per l'attuazione della disciplina NIS2, al fine di assicurare l'implementazione e attuazione del presente decreto legislativo.

L'**articolo 13** delinea la composizione ed il funzionamento del quadro nazionale di gestione delle crisi informatiche, individuando, come già anticipato, l'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore, ai sensi dell'articolo 9, paragrafo 2, della direttiva NIS2, e il Ministero della difesa, quali autorità competenti alla gestione degli incidenti e delle crisi informatiche su vasta scala (Autorità di gestione delle crisi informatiche), di cui all'articolo 9 della direttiva NIS2, ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera g). Viene quindi prevista l'adozione del ª piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scalaº, indicando anche i principali contenuti del piano stesso.

In tal senso, il comma 3 rimette la definizione del piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala ad uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale e del Ministero della difesa, ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera g), previo parere del Comitato interministeriale per la sicurezza della Repubblica nella composizione di cui all'articolo 10 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

L'**articolo 14** 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 2022-2023 che prevede di ª *o) 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;*º.

In particolare, il comma 2, lettera d), rimette ad un decreto del Presidente del Consiglio dei ministri, su proposta del Ministro della difesa, sentita l'Agenzia per la cybersicurezza nazionale, la definizione, nell'ambito dell'elenco di cui all'articolo 7, comma 2, dell'elenco dei soggetti che

impattano sulla efficienza dello Strumento militare e sulla tutela della difesa e sicurezza militare dello Stato, su cui l'Autorità nazionale competente NIS comunica tempestivamente al Ministero della difesa gli incidenti di cui all'articolo 25, nonché, con le modalità previste nello stesso decreto, le ulteriori informazioni di sicurezza cibernetica.

L'**articolo 15** 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 "*e) 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;*".

L'**articolo 16** sulla divulgazione coordinata delle vulnerabilità attribuisce allo CSIRT Italia il ruolo di coordinatore dei soggetti interessati 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, in linea con le previsioni del presente decreto e tenuto conto degli orientamenti del gruppo di cooperazione NIS.

L'**articolo 17** disciplina gli accordi di condivisione delle informazioni sulla sicurezza informatica che possono stipulare tra loro i soggetti essenziali, i soggetti importanti e i loro fornitori.

Il **Capo III** è dedicato alla cooperazione a livello dell'Unione europea e internazionale.

In particolare, all'**articolo 18** è recata la disciplina dell'attività del Gruppo di cooperazione NIS, prevedendo ± come già disponeva l'abrogando d.lgs. n. 65 del 2018 ± che l'Autorità nazionale competente NIS partecipi alle attività del gruppo di cooperazione composto da rappresentanti degli Stati membri, della Commissione europea e dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA). In tale contesto, è altresì previsto che l'Autorità nazionale competente NIS, in base allo specifico settore che di volta in volta viene in rilievo e all'ordine del giorno dei lavori delle singole riunioni, coinvolga le relative Autorità di settore NIS per la partecipazione alle riunioni e per il necessario supporto nelle attività del Gruppo.

I successivi **articoli 19** e **20** regolano, rispettivamente, la partecipazione dell'Autorità nazionale di gestione delle crisi cibernetiche alla Rete delle organizzazioni di collegamento per le crisi cibernetiche (EU-CyCLONe) e la partecipazione del CSIRT Italia alla rete di CSIRT nazionali. L'**articolo 21** introduce, quindi, la procedura di revisione tra pari, ai sensi dell'articolo 19 della direttiva NIS2, per questioni specifiche di natura transfrontaliera o intersettoriale.

L'**articolo 22**, infine, individua, successivamente all'entrata in vigore del presente decreto, gli obblighi di comunicazione nei confronti dell'Unione europea da parte della Presidenza del Consiglio dei ministri, circa la conferma dell'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente e Punto di contatto unico NIS, nonché circa la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva NIS2, e del Ministero della difesa, quali Autorità nazionali di gestione delle crisi cibernetiche, ciascuno negli ambiti di competenza indicati dal già esaminato articolo 2, comma 1, lettera g).

Il **Capo IV** è dedicato agli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente. In particolare, gli articoli 31, 32 e 33, che non corrispondono simmetricamente a puntuali disposizioni della direttiva NIS2, sono stati previsti al fine di consentire, in sede di recepimento, di declinare meglio il concetto di proporzionalità e gradualità

degli obblighi, nonché poter procedere ad un coordinamento della NIS2 con le altre normative settoriali e, in particolare, con la disciplina, di esclusiva competenza nazionale, sul Perimetro di sicurezza nazionale cibernetica di cui al decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e relativi provvedimenti di attuazione.

Con riguardo all'**articolo 23**, sono disciplinati gli obblighi e le responsabilità degli organi di amministrazione e direttivi dei soggetti essenziali e importanti, mentre nei successivi **articoli 24 e 25** sono individuati, nel dettaglio e rispettivamente, gli obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e quelli in materia di notifica di incidente. Con riferimento a tali ultimi obblighi, come prescritto dalla direttiva NIS2, sono previsti, in particolare: 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. Viene altresì introdotta, all'**articolo 26**, la possibilità di procedere alla trasmissione, su base volontaria, al CSIRT Italia di informazioni relative a incidenti, minacce informatiche e quasi incidenti, per i quali non vige l'obbligo di notifica.

L'**articolo 27**, recependo i considerando 80 e 138 della direttiva NIS2, consente all'Autorità nazionale competente NIS di imporre ai soggetti essenziali e importanti l'utilizzo di determinati prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante, ovvero acquistati da terze parti, purché siano certificati nell'ambito dei sistemi europei di certificazione della cibersicurezza. È quindi previsto che, nelle more dell'adozione, ai sensi del regolamento (UE) 2019/881 (Cybersecurity Act), dei predetti schemi di certificazione, l'Autorità nazionale competente NIS possa imporre ai soggetti essenziali e importanti di utilizzare prodotti, servizi e processi TIC che siano certificati nell'ambito di schemi di certificazione riconosciuti a livello nazionale o europeo.

L'**articolo 28** attribuisce, poi, all'Autorità nazionale competente NIS la facoltà di promuovere l'uso di specifiche tecniche per favorire l'attuazione efficace e armonizzata delle misure di gestione dei rischi di sicurezza cibernetica, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia. Al fine di dare attuazione al criterio di delega di cui all'articolo 3, comma 1, lettera h), della legge delegazione europea 2022-2023, è previsto che ACN possa redigere e aggiornare periodicamente un elenco delle tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di gestione dei rischi per la sicurezza informatica. Al fine di rendere compatibile tale previsione con quanto disposto dall'articolo 25, comma 1, della direttiva NIS2 (*ª gli Stati membri, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, incoraggiano l'uso di norme e specifiche tecniche europee e internazionali relative alla sicurezza dei sistemi informatici e di rete*º), è previsto che tale elenco non abbia carattere vincolante o esaustivo, attese le peculiari esigenze di sicurezza informatica di ciascun soggetto, e che si limiti a fornire un orientamento sulle specifiche tecniche europee e internazionali ± anche adottate da un organismo di normazione riconosciuto di cui al regolamento (UE) 1025/2012, relative alla sicurezza dei sistemi informativi e di rete ± e sulle norme di settore nazionali ed europee applicabili a ciascuno dei soggetti essenziali e importanti.

L'**articolo 29** disciplina, quindi, la banca dei dati di registrazione dei nomi di dominio.

Il successivo **articolo 30** disciplina un meccanismo di categorizzazione delle attività e dei servizi dei soggetti importanti ed essenziali, che si pone quale elemento fondante per implementare coerentemente il principio di proporzionalità nella declinazione degli obblighi previsti dalla direttiva NIS2. A tali fini, è previsto che, dal primo maggio al trenta giugno di ogni anno, a partire dalla conferma tramite piattaforma digitale dell'iscrizione nell'elenco dei soggetti importanti ed essenziali, questi, nonché i soggetti che forniscono servizi di registrazione, procedano alla

comunicazione e all'aggiornamento di un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione ai fini della relativa categorizzazione.

Sebbene la direttiva NIS2 non stabilisca i termini entro cui i soggetti essenziali e importanti sono tenuti ad effettuare tale comunicazione, l'articolo 30 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.

L'**articolo 31** stabilisce che l'Autorità nazionale competente NIS preveda obblighi in materia di gestione del rischio di sicurezza cibernetica e di notifica di incidente, proporzionati anche 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. La norma attribuisce poi alla medesima Autorità il potere di stabilire termini, modalità, specifiche e tempi graduali di implementazione dei suddetti obblighi, anche ai sensi del combinato disposto dei considerando 15 e 81 della direttiva NIS2.

L'**articolo 32** detta regole specifiche per le pubbliche amministrazioni e per i soggetti essenziali e importanti che forniscono servizi, anche digitali, alle medesime, in linea con quanto prescritto dai considerando 85 e 130 della direttiva NIS2.

L'**articolo 33**, infine, prevede disposizioni di coordinamento della normativa NIS2 con la sopra richiamata disciplina del Perimetro di sicurezza nazionale cibernetica. In particolare, con riferimento ai soggetti inseriti nell'elenco di cui all'articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019, (i c.d. ªsoggetti perimetroº) e, nello specifico, in relazione alle sole reti e ai soli sistemi informativi e servizi informatici da cui dipendono l'esercizio di quelle funzioni essenziali dello Stato, ovvero la prestazione di quei servizi essenziali per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, in relazione ai quali i soggetti sono stati inseriti nel Perimetro, è previsto che trovino applicazione gli obblighi e le misure previsti dal decreto-legge n. 105 del 2019 e indicati dal medesimo articolo 33. Ciò considerando il peculiare ambito di operatività delle disposizioni in parola, che attengono direttamente alla tutela della sicurezza nazionale nello spazio cibernetico e che, pertanto, rientrano nei casi di esclusiva competenza di ciascuno Stato membro ai sensi dell'articolo 4, paragrafo 2, del Trattato sull'Unione europea.

Il **Capo V**, dedicato alle funzioni e attività di monitoraggio, vigilanza ed esecuzione, recepisce il Capo VII della direttiva NIS2 dedicato a ªVigilanza ed esecuzioneº e propone un sistema di supervisione più confacente alle attività svolte da ACN, con l'individuazione delle diverse fasi e degli strumenti di cui l'Autorità nazionale competente NIS può disporre. In particolare, si è proceduto a distinguere una prima fase di monitoraggio, analisi e supporto (articolo 35), che agevola la conoscenza del soggetto da parte di ACN e l'acquisizione corretta delle informazioni che lo riguardano; una seconda fase, di verifiche e ispezioni, che disciplina l'esercizio da parte dell'Autorità nazionale competente NIS dei suoi poteri di accertamento e ispettivi (articolo 36); una terza fase, di esecuzione (articolo 37), nella quale l'Autorità nazionale competente NIS, ove necessario e all'esito delle prime due fasi dell'attività di monitoraggio e vigilanza, può disporre istruzioni vincolanti e, in caso di inottemperanza, espresse diffide a porre in essere gli adempimenti richiesti; una quarta fase, infine, sulle sanzioni amministrative, con la previsione anche di misure deflattive del contenzioso (articolo 38). Come previsto dalla direttiva NIS2, istruzioni e diffide garantiscono ± anche in base ai principi generali introdotti dall'articolo 35 ± i diritti del soggetto alla produzione di documenti e memorie e all'indicazione di modalità e termini ragionevoli e proporzionati per adempiere, o riferire circa lo stato di implementazione delle disposizioni impartite.

In particolare, all'**articolo 34**, sono disciplinati gli aspetti generali relativi alle attività di monitoraggio, analisi e supporto, di verifica ed ispezione, nonché all'adozione di misure di esecuzione e all'irrogazione delle sanzioni, attribuendo all'Autorità nazionale competente NIS la supervisione sull'adempimento degli obblighi previsti dalla direttiva NIS2 e sui relativi effetti in materia di sicurezza dei sistemi informativi e di rete da parte dei soggetti essenziali e dei soggetti importanti.

Gli **articoli 35, 36, 37 e 38** prevedono, in particolare e ulteriormente, che l'Autorità nazionale competente NIS garantisca un'attività di monitoraggio, analisi e supporto ai soggetti sulla base delle informazioni e delle eventuali rendicontazioni trasmesse; eserciti i poteri di verifica e ispettivi ± relativi agli obblighi cui sono sottoposti, rispettivamente, i soggetti essenziali ed importanti ±; adotti misure di esecuzione per una corretta implementazione della direttiva NIS2 e individui i criteri e le modalità di irrogazione delle sanzioni ai soggetti essenziali e importanti, affinché le stesse risultino effettive, proporzionate e dissuasive rispetto alle eventuali violazioni, in linea con quanto stabilito dall'articolo 3, comma 1, lettera n), numero 1), della legge di delegazione europea 2022-2023, che dispone di ª n) *rivedere il sistema sanzionatorio e il sistema di vigilanza ed esecuzione, in particolare: 1) prevedendo sanzioni effettive, proporzionate e dissuasive rispetto alla gravità della violazione degli obblighi derivanti dalla direttiva (UE) 2022/2555, anche in deroga ai criteri e ai limiti previsti dall@articolo 32, comma 1, lettera d), della legge 24 dicembre 2012, n. 234, e alla legge 24 novembre 1981, n. 689, introducendo strumenti deflativi del contenzioso, quali la diffida ad adempiere;*º .

In tale ambito, è stato declinato il principio di proporzionalità stabilito dalla direttiva NIS2 e, al contempo, è stato limitato il rischio di esporre il tessuto produttivo nazionale a un regime sperequativo rispetto a quello adottato dagli altri Stati membri, che potrebbe danneggiare le imprese italiane e rendere meno attrattivo il Paese per realtà produttive straniere. Per conseguire tale obiettivo, le fattispecie delle violazioni elencate all'articolo 38 dello schema in oggetto sono state suddivise in due diverse fasce, valorizzando quanto previsto dall'articolo 34 della direttiva NIS2, che stabilisce l'applicazione del massimo edittale solo per l'inosservanza degli obblighi di gestione del rischio per la sicurezza informatica e di notifica di incidente di cui agli articoli 21 e 23 della stessa direttiva. In particolare, nella prima fascia sono state ricomprese le cennate violazioni, cui sono state aggiunte quelle relative alla inosservanza degli obblighi posti in capo agli organi di amministrazione e direttivi. Tali condotte sono punite con sanzioni pecuniarie fino a 10.000.000 di euro per i soggetti essenziali, ovvero il 2% del fatturato, se superiore, il cui minimo è fissato nella misura di un ventesimo del massimo edittale, e fino a 7.000.000 di euro per quelli importanti, ovvero il 1,4% del fatturato, se superiore, il cui minimo è fissato nella misura di un trentesimo del massimo edittale. La seconda fascia ricomprende tutte le altre condotte per le quali la direttiva NIS2 non determina l'importo della sanzione applicabile, demandando tale definizione agli Stati membri. In tali casi, analogamente a quanto fatto dall'Austria e dal Belgio, vengono applicate sanzioni pecuniarie amministrative di entità sensibilmente inferiore. L'articolo 38 prevede anche, al comma 15, strumenti deflattivi del contenzioso in ottemperanza a quanto disposto dall'articolo 3, lettera n), punto 1), della legge di delegazione europea 2022-2023, costituiti (lettera *a*) da un ª invito a conformarsiº alla normativa vigente, inviata al trasgressore dall'Autorità nazionale competente NIS, e (lettera *b*) dalla possibilità, rimessa sempre al trasgressore, di accedere al pagamento della sanzione in misura ridotta.

Con specifico riferimento, invece, alla Pubblica Amministrazione, la direttiva NIS2 lascia agli Stati membri la libertà di decidere se applicare o meno sanzioni a tali soggetti, e nella eventuale definizione dei minimi e dei massimi edittali. In un'ottica di omogeneità del quadro normativo nazionale in materia di cybersicurezza si è, pertanto, optato per l'irrogazione di sanzioni pecuniarie da 25.000 a 125.000 euro per le violazioni più gravi, di cui al comma 8 dell'articolo 38, e da 10.000

a 50.000 euro per tutte le altre violazioni, definite al comma 10 del medesimo articolo. È altresì previsto che tali sanzioni vengano ridotte di un terzo per le Pubbliche Amministrazioni individuate come soggetti importanti e, al comma 14, che la mancata notifica sia punita con sanzioni amministrative solo in caso di reiterazione nell'arco di un periodo di tempo fissato in cinque anni.

Infine, 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 in materia di supervisione.

Il **Capo VI** è, infine, dedicato alle disposizioni finali e transitorie.

All'**articolo 40**, per finalità di razionalizzazione e maggiore chiarezza del testo, nonché per agevolare l'implementazione della nuova normativa, e secondo un criterio di individuazione delle fonti sulla base della materia da disciplinare, sono state dettate le disposizioni relative alla quasi totalità dei provvedimenti di attuazione del presente decreto, che dovranno essere adottati dal Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale, sentiti, o d'intesa con, a seconda del provvedimento, il Tavolo per l'attuazione della disciplina NIS, le Autorità di settore NIS interessate e le altre eventuali Amministrazioni interessate, previo parere del Comitato interministeriale per la cybersicurezza. È altresì prevista l'adozione di determinazioni dell'Agenzia per la cybersicurezza nazionale, da adottarsi su proposta delle Autorità di settore NIS interessate, e sentito il Tavolo per l'attuazione della disciplina NIS.

L'**articolo 41** dispone l'abrogazione del d.lgs. n. 65 del 2018 di recepimento della prima direttiva NIS e degli articoli 40 (ª Sicurezza delle reti e dei servizi º) e 41 (ª Attuazione e controllo º) del d.lgs. n. 259 del 2003 recante ª Codice delle comunicazioni elettroniche º, 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.

Il successivo **articolo 42** regola la prima fase di applicazione del presente decreto legislativo ai fornitori di servizi DNS, ai registri dei nomi di dominio di primo livello, ai soggetti che forniscono servizi di registrazione dei nomi di dominio, ai fornitori di servizi di cloud computing, di data center, di reti di distribuzione dei contenuti, di servizi gestiti, di servizi di sicurezza gestiti, nonché ai fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network. L'articolo inoltre, detta specifiche disposizioni circa la fase di prima applicazione dell'obbligo di registrazione dei soggetti essenziali e importanti, delle modalità di convocazione del Tavolo per l'attuazione della disciplina NIS e per l'implementazione dell'obbligo di elencazione, caratterizzazione e categorizzazione delle attività e dei servizi altamente critici e critici. Vengono inoltre stabiliti termini massimi, per il primo adeguamento dei soggetti essenziali importanti alla declinazione di base degli obblighi previsti dalla direttiva NIS2, fissati in 9 mesi per quelli di cui all'articolo 25, relativi alle notifiche di incidente, e 18 mesi per gli altri obblighi di cui agli articoli 23, 24 e 29.

L'**articolo 43** introduce alcune modifiche alla disciplina nazionale in materia di sicurezza cibernetica in linea con quanto disposto dall'articolo 3, comma 1, lettera p), della legge di delegazione europea 2022-2023 che prevede, come già evidenziato, di ª *apportare alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il coordinamento con le disposizioni emanate in attuazione º* dello stesso articolo 3.

L'**articolo 44**, infine, reca le disposizioni finanziarie necessarie per far fronte agli oneri derivanti dall'attuazione del presente decreto legislativo.

DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DEL 14 DICEMBRE 2022 RELATIVA A MISURE PER UN LIVELLO COMUNE ELEVATO DI CIBERSICUREZZA 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)	**SCHEMA DI DECRETO LEGISLATIVO di recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148** **ARTICOLO 3 LEGGE 21 FEBBRAIO 2024, N. 15 - LEGGE DI DELEGAZIONE EUROPEA 2022-2023**
CAPO I **Disposizioni generali**	**CAPO I** **Disposizioni generali**
Articolo 1 **Oggetto e ambito di applicazione** 1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno. 2. A tal fine, la presente direttiva stabilisce: a) obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT); b) misure in materia di gestione dei rischi di cibersicurezza e obblighi di segnalazione per i soggetti di un tipo di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557; c) norme e obblighi in materia di condivisione delle informazioni sulla cibersicurezza; d) obblighi in materia di vigilanza ed esecuzione per gli Stati membri.	**ART. 1** ***(Oggetto)***

Articolo 2 Ambito di applicazione	ART. 3 *(Ambito di applicazione)*
1. La presente direttiva si applica ai soggetti pubblici o privati delle tipologie di cui all'allegato I o II che sono considerati medie imprese ai sensi all'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superano i massimali per le medie imprese di cui al paragrafo 1 di tale articolo, e che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione. L'articolo 3, paragrafo 4, dell'allegato a tale raccomandazione non si applica ai fini della presente direttiva. 2. La presente direttiva si applica anche ai soggetti, indipendentemente dalle loro dimensioni, delle tipologie di cui all'allegato I o II qualora: a) i servizi siano forniti da: i) fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico; ii) prestatore di servizi di fiducia; iii) registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio; b) il soggetto sia l'unico fornitore in uno Stato membro 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 regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro; f) il soggetto è un ente della pubblica amministrazione:	

i) dell'amministrazione centrale quale definito da uno Stato membro conformemente al diritto nazionale; o ii) a livello regionale quale definito da uno Stato membro conformemente al diritto nazionale che, a seguito di una valutazione basata sul rischio, fornisce servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche. 3. La presente direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557. 4. La presente direttiva si applica ai soggetti, indipendentemente dalle loro dimensioni, che forniscono servizi di registrazione dei nomi di dominio. 5. Gli Stati membri possono prevedere che la presente direttiva si applichi a: a) enti della pubblica amministrazione a livello locale; b) istituti di istruzione, in particolare ove svolgano attività di ricerca critiche.	
6. La presente direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico. 7. La presente direttiva non si applica agli enti della pubblica amministrazione 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. 8. Gli Stati membri possono esentare soggetti specifici che svolgono attività nei settori della sicurezza nazionale, della pubblica sicurezza, della difesa o del contrasto, compresi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, o che forniscono servizi esclusivamente agli enti della pubblica amministrazione di cui al paragrafo 7 del presente articolo, dal rispetto degli obblighi di cui all'articolo 21 o all'articolo 23 per quanto riguarda tali attività o servizi. In tali casi, le	**ART. 4** ***(Protezione degli interessi nazionali e commerciali)***

misure di vigilanza e di applicazione di cui al capo VII non si applicano in relazione a tali attività o servizi specifici. Qualora i soggetti svolgano attività o prestino servizi esclusivamente del tipo di cui al presente paragrafo, gli Stati membri possono anche decidere di esentare tali enti dagli obblighi di cui agli articoli 3 e 27. 9. I paragrafi 7 e 8 non si applicano quando un soggetto agisce in qualità di prestatore di servizi fiduciari. 10. La presente direttiva non si applica ai soggetti che gli Stati membri hanno esentato dall'ambito di applicazione del regolamento (UE) 2022/2554 ai sensi dell'articolo 2, paragrafo 4, di tale regolamento. 11. Gli obblighi stabiliti nella presente direttiva non comportano la fornitura di informazioni la cui divulgazione sia contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa. 12. La presente direttiva si applica fatti salvi il regolamento (UE) 2016/679, la direttiva 2002/58/CE, le direttive 2011/93/UE (27) e 2013/40/UE (28) del Parlamento europeo e del Consiglio e la direttiva (UE) 2022/2557. 13. Fatto salvo l'articolo 346 TFUE, le informazioni riservate ai sensi della normativa dell'Unione o nazionale, quale quella sulla riservatezza commerciale, sono scambiate con la Commissione e con altre autorità competenti conformemente alla presente direttiva solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione della presente direttiva. Le informazioni scambiate sono limitate alle informazioni pertinenti e commisurate a tale scopo. Lo scambio di informazioni tutela la riservatezza di dette informazioni e protegge la sicurezza e gli interessi commerciali di soggetti interessati. 14. I soggetti, le autorità competenti, i punti di contatto unici e i CSIRT trattano i dati personali nella misura necessaria ai fini della presente direttiva e conformemente al regolamento (UE) 2016/679, in particolare tale trattamento si basa sull'articolo 6 dello stesso. Il trattamento dei dati personali a norma della presente direttiva da parte dei fornitori di reti pubbliche di comunicazione elettronica o dei	**ART. 8** ***(Protezione dei dati personali)***

fornitori di comunicazioni elettroniche accessibili al pubblico viene effettuato in conformità della legislazione dell'Unione in materia di protezione dei dati e della legislazione dell'Unione in materia di riservatezza, segnatamente la direttiva 2002/58/CE.	
Articolo 3 **Soggetti essenziali e importanti** 1. Ai fini della presente direttiva, sono considerati soggetti essenziali i seguenti: a) soggetti di cui all'allegato I che superano i massimali per le medie imprese di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE; b) prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni; c) fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese ai sensi dell'articolo 2, dell'allegato alla raccomandazione 2003/361/CE; d) i soggetti della pubblica amministrazione di cui all'articolo 2, paragrafo 2, lettera f), punto i); e) qualsiasi altro soggetto di cui all'allegato I o II che uno Stato membro identifica come soggetti essenziali ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e); f) soggetti identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557, di cui all'articolo 2, paragrafo 3 della presente direttiva; g) se lo Stato membro lo prevede, i soggetti che tale Stato membro ha identificato prima del 16 gennaio 2023 come operatori di servizi essenziali a norma della direttiva (UE) 2016/1148 o del diritto nazionale. 2. Ai fini della presente direttiva, sono considerati soggetti importanti i soggetti di una tipologia elencata negli allegati I o II che non sono considerati soggetti essenziali ai sensi del paragrafo 1 del presente articolo. Ciò comprende soggetti identificati dagli Stati membri come soggetti importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);	**ART. 6** ***(Soggetti essenziali e importanti)***

3. Entro il 17 aprile 2025, gli Stati membri definiscono un elenco dei soggetti essenziali ed importanti nonché dei soggetti che forniscono servizi di registrazione dei nomi di dominio. Successivamente, gli Stati membri riesaminano l'elenco periodicamente, almeno ogni due anni e, se opportuno, lo aggiornano. 4. Ai fini della compilazione dell'elenco di cui al paragrafo 3, gli Stati membri impongono alle entità di cui a tale paragrafo di presentare alle autorità competenti almeno le informazioni seguenti: a) il proprio nome; b) l'indirizzo e i recapiti aggiornati, compresi gli indirizzi e-mail, le serie di IP e i numeri di telefono; c) se del caso, i settori e sottosettori pertinenti di cui all'allegato I o II; e d) se del caso, un elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione della presente direttiva. I soggetti di cui al paragrafo 3 notificano tempestivamente qualsiasi modifica delle informazioni trasmesse a norma del primo comma del presente paragrafo e in ogni caso entro due settimane dalla data della modifica. La Commissione, assistita dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA), fornisce senza indebito ritardo orientamenti e modelli relativi agli obblighi di cui al presente paragrafo. Gli Stati membri possono istituire meccanismi nazionali che consentano alle entità di registrarsi. 5. Entro il 17 aprile 2025 e successivamente ogni due anni, le autorità competenti notificano: a) alla Commissione e al gruppo di coordinamento, il numero dei soggetti essenziali e importanti elencati ai sensi del paragrafo 3 per ciascun settore e sottosettore di cui all'allegato I o II; e b) alla Commissione informazioni pertinenti sul numero di soggetti essenziali e importanti individuati ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e), sul settore e il sottosettore di cui all'allegato I o II cui appartengono, sul tipo di servizio che forniscono e sulla fornitura, tra quelli stabiliti all'articolo 2, paragrafo 2, lettere	**ART. 7** ***(Identificazione ed elencazione dei soggetti essenziali e importanti)***

da b) a e), ai sensi dei quali sono stati individuati. 6. Sino al 17 aprile 2025 e su richiesta della Commissione, gli Stati membri possono notificare alla Commissione i nomi dei soggetti essenziali e importanti di cui al paragrafo 5, lettera b).	
Articolo 4 **Atti giuridici settoriali dell'Unione** 1. Qualora gli atti giuridici settoriali dell'Unione facciano obbligo ai soggetti essenziali o importanti di adottare misure di gestione dei rischi di cibersicurezza o di notificare gli incidenti significativi, nella misura in cui gli effetti di tali obblighi siano almeno equivalenti a quelli degli obblighi di cui alla presente direttiva, a tali soggetti non si applicano le pertinenti disposizioni della presente direttiva, comprese le disposizioni relative alla vigilanza e all'esecuzione di cui al capo VII. Qualora gli atti giuridici settoriali dell'Unione non contemplino tutti i soggetti di un settore specifico che rientra nell'ambito di applicazione della presente direttiva, le pertinenti disposizioni della presente direttiva continuano ad applicarsi ai soggetti non contemplati da tali atti giuridici settoriali dell'Unione. 2. I requisiti di cui al paragrafo 1 del presente articolo sono considerati di effetto equivalente agli obblighi stabiliti dalla presente direttiva qualora: a) gli effetti delle misure di gestione dei rischi di cibersicurezza siano almeno equivalenti a quelli delle misure di cui all'articolo 21, paragrafi 1 e 2; oppure b) l'atto giuridico settoriale dell'Unione preveda l'accesso immediato, se del caso automatico e diretto, alle notifiche degli incidenti da parte dei CSIRT, delle autorità competenti o dei punti di contatto unici a norma della presente direttiva e qualora gli obblighi di notifica degli incidenti significativi abbiano un effetto almeno equivalente a quelli di cui all'articolo 23, paragrafi da 1 a 6, della presente direttiva. 3. La Commissione, entro il 17 luglio 2023, fornisce orientamenti che chiariscano l'applicazione dei paragrafi 1 e 2. La Commissione rivede tali orientamenti periodicamente. Nella preparazione di detti	*Recepimento non richiesto*

orientamenti, la Commissione tiene conto delle osservazioni del gruppo di cooperazione e dell'ENISA.	
Articolo 5 **Armonizzazione minima** La presente direttiva non impedisce agli Stati membri di adottare o mantenere disposizioni che garantiscano un livello più elevato di cibersicurezza, a condizione che tali disposizioni siano coerenti con gli obblighi degli Stati membri stabiliti dal diritto dell'Unione.	*Recepimento non richiesto*
Articolo 6 **Definizioni** Ai fini della presente direttiva si applicano le definizioni seguenti: 1) «sistema informatico e di rete»: a) una rete di comunicazione elettronica quale definita all'articolo 2, punto 1, della direttiva (UE) 2018/1972; b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base a un programma, un'elaborazione automatica di dati digitali; o c) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo degli elementi di cui alle lettere a) e b), ai fini del loro funzionamento, del loro uso, della loro protezione e della loro manutenzione; 2) «sicurezza dei sistemi informatici e di rete»: la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi; 3) «cibersicurezza»: la cibersicurezza quale definita all'articolo 2, punto 1), del regolamento (UE) 2019/881; 4) «strategia nazionale per la cibersicurezza»: un quadro coerente di uno Stato membro che prevede priorità e obiettivi strategici in materia di cibersicurezza e la governance per il loro conseguimento in tale Stato membro;	**Articolo 2** **(Definizioni)**

5) «quasi incidente»: un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato; 6) «incidente»: 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 informatici e di rete o accessibili attraverso di essi; 7) «incidente di cibersicurezza su vasta scala»: un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri; 8) «gestione degli incidenti»: le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e riprendersi da esso; 9) «rischio»: la potenziale perdita o perturbazione causata da un incidente; è espresso come combinazione dell'entità di tale perdita o perturbazione e della probabilità che l'incidente si verifichi; 10) «minaccia informatica»: una minaccia informatica quale definita all'articolo 2, punto 8), del regolamento (UE) 2019/881; 11) «minaccia informatica significativa»: una minaccia informatica che, in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informatici e di rete di un soggetto o degli utenti di tali servizi del soggetto causando perdite materiali o immateriali considerevoli; 12) «prodotto TIC»: un prodotto TIC quale definito all'articolo 2, punto 12), del regolamento (UE) 2019/881; 13) «servizio TIC»: un servizio TIC quale definito all'articolo 2, punto 13), del regolamento (UE) 2019/881; 14) «processo TIC»: un processo TIC quale definito all'articolo 2, punto 14), del regolamento (UE) 2019/881; 15) «vulnerabilità»: un punto debole, una suscettibilità o un difetto di prodotti TIC o	

servizi TIC che può essere sfruttato da una minaccia informatica; 16) «norma»: una norma quale definita all'articolo 2, punto 1), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio; 17) «specifica tecnica»: una specifica tecnica quale definita all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012; 18) «punto di interscambio internet»: un'infrastruttura di rete che consente l'interconnessione di più di due reti indipendenti (sistemi autonomi), principalmente al fine di agevolare lo scambio del traffico internet, che fornisce interconnessione soltanto ai sistemi autonomi e che non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo né altera o interferisce altrimenti con tale traffico; 19) «sistema dei nomi di dominio» o «DNS»: un sistema di nomi gerarchico e distribuito che consente l'identificazione di servizi e risorse su internet, permettendo ai dispositivi degli utenti finali di utilizzare i servizi di inoltro e connettività di internet al fine di accedere a tali servizi e risorse; 20) «fornitore di servizi DNS»: un soggetto che fornisce: a) servizi di risoluzione dei nomi di dominio ricorsivi accessibili al pubblico per gli utenti finali di internet; o b) servizi di risoluzione dei nomi di dominio autorevoli per uso da parte di terzi, fatta eccezione per i server dei nomi radice; 21) «registro dei nomi di dominio di primo livello» o «registro dei nomi TLD»: un soggetto cui è stato delegato uno specifico dominio di primo livello (TLD) e che è responsabile dell'amministrazione di tale TLD, compresa la registrazione dei nomi di dominio sotto tale TLD, e del funzionamento tecnico di tale TLD, compresi il funzionamento dei server dei nomi, la manutenzione delle banche dati e la distribuzione dei file di zona TLD tra i server dei nomi, indipendentemente dal fatto che una qualsiasi di tali operazioni sia effettuata dal soggetto stesso o sia esternalizzata, ma escludendo le situazioni in cui i nomi TLD sono	

utilizzati da un registro esclusivamente per uso proprio; 22) «soggetto che fornisce servizi di registrazione di nomi di dominio»: 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; 23) «servizio digitale»: un servizio quale definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio; 24) «servizio fiduciario»: un servizio fiduciario quale definito all'articolo 3, punto 16), del regolamento (UE) n. 910/2014; 25) «prestatore di servizi fiduciari»: un prestatore di servizi fiduciari quale definito all'articolo 3, punto 19), del regolamento (UE) n. 910/2014; 26) «servizio fiduciario qualificato»: un servizio fiduciario qualificato quale definito all'articolo 3, punto 17), del regolamento (UE) n. 910/2014; 27) «prestatore di servizi fiduciari qualificato»: un prestatore di servizi fiduciari qualificato quale definito all'articolo 3, punto 20), del regolamento (UE) n. 910/2014; 28) «mercato online»: un mercato online quale definito all'articolo 2, lettera n), della direttiva 2005/29/CE del Parlamento europeo e del Consiglio; 29) «motore di ricerca online»: un motore di ricerca online quale definito all'articolo 2, punto 5), del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio; 30) «servizio di cloud computing»: un servizio digitale che consente l'amministrazione su richiesta di un pool scalabile ed elastico di risorse di calcolo condivisibili e l'ampio accesso remoto a quest'ultimo, anche ove tali risorse sono distribuite in varie ubicazioni. 31) «servizio di data center»: un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare, interconnettere e far funzionare in modo centralizzato apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale;	

32) «rete di distribuzione dei contenuti (*content delivery network*)»: una rete di server distribuiti geograficamente allo scopo di garantire l'elevata disponibilità, l'accessibilità o la rapida distribuzione di contenuti e servizi digitali agli utenti di internet per conto di fornitori di contenuti e servizi; 33) «piattaforma di servizi di social network»: una piattaforma che consente agli utenti finali di entrare in contatto, condividere, scoprire e comunicare gli uni con gli altri su molteplici dispositivi, in particolare, attraverso chat, post, video e raccomandazioni; 34) «rappresentante»: una persona fisica o giuridica stabilita nell'Unione espressamente designata ad agire per conto di un fornitore di servizi DNS, un registro dei nomi TLD, un soggetto che fornisce servizi di registrazione di nomi di dominio, un fornitore di servizi di cloud computing, un fornitore di servizi di data center, un fornitore di reti di distribuzione dei contenuti, un fornitore di servizi gestiti, un fornitore di servizi di sicurezza gestiti, o un fornitore di mercato online, di un motore di ricerca online o di una piattaforma di servizi di social network che non è stabilito nell'Unione, a cui l'autorità nazionale competente o un CSIRT può rivolgersi in luogo del soggetto per quanto riguarda gli obblighi di quest'ultimo a norma della presente direttiva; 35) «ente della pubblica amministrazione»: un soggetto riconosciuto come tale in uno Stato membro conformemente al diritto nazionale, che non comprende la magistratura, i parlamenti e le banche centrali, che soddisfa i criteri seguenti: a) è istituito allo scopo di soddisfare esigenze di interesse generale e non ha carattere industriale o commerciale; b) è dotato di personalità giuridica o è autorizzato per legge ad agire a nome di un altro soggetto dotato di personalità giuridica; c) è finanziato in modo maggioritario dallo Stato, da autorità regionali o da altri organismi di diritto pubblico, la sua gestione è soggetta alla vigilanza di tali autorità o organismi, oppure è dotato di un organo di amministrazione, di direzione o di vigilanza in cui più della metà dei	

membri è designata dallo Stato, da autorità regionali o da altri organismi di diritto pubblico; d) ha il potere di adottare, nei confronti di persone fisiche o giuridiche, decisioni amministrative o normative che incidono sui loro diritti relativi alla circolazione transfrontaliera delle merci, delle persone, dei servizi o dei capitali; 36) «rete pubblica di comunicazione elettronica»: una rete pubblica di comunicazione elettronica quale definita all'articolo 2, punto 8), della direttiva (UE) 2018/1972; 37) «servizio di comunicazione elettronica»: un servizio di comunicazione elettronica quale definito all'articolo 2, punto 4), della direttiva (UE) 2018/1972; 38) «soggetto»: una persona fisica o giuridica, costituita e riconosciuta come tale conformemente al diritto nazionale applicabile nel suo luogo di stabilimento, che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi; 39) «fornitore di servizi gestiti»: un soggetto che fornisce servizi relativi all'installazione, alla gestione, al funzionamento o alla manutenzione di prodotti, reti, infrastrutture, applicazioni TIC o di qualsiasi altro sistema informatico e di rete, tramite assistenza o amministrazione attiva effettuata nei locali dei clienti o a distanza; 40) «fornitore di servizi di sicurezza gestiti»: un fornitore di servizi di sicurezza gestiti che svolge o fornisce assistenza per attività relative alla gestione dei rischi di cibersicurezza; 41) «organismo di ricerca»: un soggetto che ha come obiettivo principale lo svolgimento di attività di ricerca applicata o di sviluppo sperimentale al fine di sfruttare i risultati di tale ricerca a fini commerciali, ma che non comprende gli istituti di istruzione.	
CAPO II **QUADRI COORDINATI IN MATERIA DI CIBERSICUREZZA**	**CAPO II** **QUADRO NAZIONALE DI SICUREZZA INFORMATICA**
Articolo 7 **Strategia nazionale per la cibersicurezza** 1. Ogni Stato membro adotta una strategia nazionale per la cibersicurezza che prevede gli	**ART. 9** ***(Strategia nazionale di cybersicurezza)***

obiettivi strategici e le risorse necessarie per conseguirli, nonché adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cibersicurezza. La strategia nazionale per la cibersicurezza comprende: a) gli obiettivi e le priorità della strategia per la cibersicurezza dello Stato membro, che riguardano in particolare i settori di cui agli allegati I e II; b) un quadro di governance per la realizzazione degli obiettivi e delle priorità di cui alla lettera a) del presente paragrafo, comprendente le misure strategiche di cui al paragrafo 2; c) un quadro di governance che chiarisca i ruoli e le responsabilità dei pertinenti portatori di interessi a livello nazionale, a sostegno della cooperazione e del coordinamento a livello nazionale tra le autorità competenti, i punti di contatto unici e i CSIRT ai sensi della presente direttiva, nonché il coordinamento e la cooperazione tra tali organismi e le autorità competenti ai sensi degli atti giuridici settoriali dell'Unione; d) un meccanismo per individuare le risorse e una valutazione dei rischi nello Stato membro in questione; e) l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato; f) un elenco delle diverse autorità e dei diversi portatori di interessi coinvolti nell'attuazione della strategia nazionale per la cibersicurezza; g) un quadro strategico per il rafforzamento del coordinamento tra le autorità competenti a norma della presente direttiva e le autorità competenti a norma della direttiva (UE) 2022/2557 ai fini della condivisione delle informazioni sui rischi, le minacce e gli incidenti sia informatici che non informatici e dello svolgimento di compiti di vigilanza, se del caso; h) un piano, comprendente le misure necessarie, per aumentare livello generale di consapevolezza dei cittadini in materia di cibersicurezza.	

2. Nell'ambito della strategia nazionale per la cibersicurezza, gli Stati membri adottano in particolare misure strategiche riguardanti: a) la cibersicurezza nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati da soggetti per la fornitura dei loro servizi; b) l'inclusione e la definizione di requisiti concernenti la cibersicurezza per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cibersicurezza, alla cifratura e l'utilizzo di prodotti di cibersicurezza open source; c) la gestione delle vulnerabilità, ivi comprese la promozione e l'agevolazione della divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12, paragrafo 1; d) il sostegno della disponibilità generale, dell'integrità e della riservatezza del carattere fondamentale pubblico di una rete internet aperta, compresa, se del caso, la cibersicurezza dei cavi di comunicazione sottomarini; e) la promozione dello sviluppo e dell'integrazione di tecnologie avanzate pertinenti miranti ad attuare misure di avanguardia nella gestione dei rischi di cibersicurezza; f) la promozione e lo sviluppo di attività di istruzione, formazione e sensibilizzazione, di competenze e di iniziative di ricerca e sviluppo in materia di cibersicurezza, nonché orientamenti sulle buone pratiche e sui controlli concernenti l'igiene informatica, destinati ai cittadini, ai portatori di interessi e ai soggetti; g) il sostegno agli istituti accademici e di ricerca volto a sviluppare, rafforzare e promuovere la diffusione di strumenti di cibersicurezza e di infrastrutture di rete sicure; h) la messa a punto di procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni sulla cibersicurezza tra soggetti, nel rispetto del diritto dell'Unione; i) il rafforzamento dei valori di riferimento relativi alla ciberresilienza e all'igiene informatica delle PMI, in particolare quelle escluse dall'ambito di applicazione della presente direttiva, fornendo orientamenti e	

sostegno facilmente accessibili per le loro esigenze specifiche; j) la promozione di una protezione informatica attiva. 3. Gli Stati membri notificano le loro strategie nazionali per la cibersicurezza alla Commissione entro tre mesi dall'adozione. Gli Stati membri possono omettere dalla notifica informazioni relative alla propria sicurezza nazionale. 4. Gli Stati membri valutano le proprie strategie nazionali per la cibersicurezza periodicamente e almeno ogni cinque anni sulla base di indicatori chiave di prestazione e, se necessario, le aggiornano. L'ENISA assiste gli Stati membri, su richiesta di questi ultimi, nell'elaborazione o aggiornamento di una strategia nazionale per la cibersicurezza e di indicatori chiave di prestazione per la relativa valutazione, onde allinearla ai requisiti e agli obblighi di cui alla presente direttiva.	
Articolo 8 **Autorità competenti e punti di contatto unici** 1. Ogni Stato membro designa o istituisce una o più autorità competenti responsabili della cibersicurezza e dei compiti di vigilanza di cui al capo VII (autorità competenti). 2. Le autorità competenti di cui al paragrafo 1 controllano l'attuazione della presente direttiva a livello nazionale. 3. Ogni Stato membro designa o istituisce un punto di contatto unico. Se uno Stato membro designa o istituisce soltanto un'autorità competente a norma del paragrafo 1, quest'ultima è anche il punto di contatto unico per tale Stato membro. 4. 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'ENISA, nonché per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro. 5. Gli Stati membri garantiscono che le proprie autorità competenti e i propri punti di contatto unici siano dotati di risorse adeguate per svolgere in modo efficiente ed efficace i compiti	**ART. 10** ***(Autorità nazionale competente e Punto di contatto unico)***

loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva. 6. Ogni Stato membro notifica alla Commissione, senza indebiti ritardi, l'identità dell'autorità competente di cui al paragrafo 1 e del punto di contatto unico di cui al paragrafo 3, i compiti di tali autorità e qualsiasi ulteriore modifica dei medesimi. Ciascuno Stato membro rende pubblica l'identità della propria autorità competente. La Commissione elabora un elenco dei punti di contatto unici disponibili.	**ART. 22** ***(Comunicazioni all'Unione europea)***
Articolo 9 **Quadri nazionali di gestione delle crisi informatiche** 1. Ogni Stato membro designa o istituisce una o più autorità competenti responsabili della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala (autorità di gestione delle crisi informatiche). Gli Stati membri provvedono affinché tali autorità dispongano di risorse adeguate per svolgere i compiti loro assegnati in modo efficace ed efficiente. Gli Stati membri assicurano la coerenza con i quadri nazionali esistenti di gestione generale delle crisi. 2. Se uno Stato membro designa o istituisce più di un'autorità di gestione delle crisi informatiche ai sensi del paragrafo 1, esso indica chiaramente quale di tali autorità deve fungere da coordinatore per la gestione di incidenti e crisi di cibersicurezza su vasta scala. 3. Ogni Stato membro individua le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi ai fini della presente direttiva. 4. Ogni Stato membro adotta un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala in cui sono stabiliti gli obiettivi e le modalità della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala. In tale piano sono definiti, in particolare: a) gli obiettivi delle misure e delle attività nazionali di preparazione; b) i compiti e le responsabilità delle autorità di gestione delle crisi informatiche; c) le procedure di gestione delle crisi informatiche, tra cui la loro integrazione nel	**ART. 13** **(Quadro nazionale di gestione delle crisi informatiche)**

quadro nazionale generale di gestione delle crisi 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 dello Stato membro alla gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala a livello dell'Unione. 5. Entro tre mesi dalla designazione o istituzione dell'autorità di gestione delle crisi informatiche di cui al paragrafo 1, ciascuno Stato membro notifica alla Commissione l'identità della propria autorità e qualsiasi ulteriore modifica alla stessa. Gli Stati membri presentano alla Commissione e alla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) le informazioni pertinenti relative ai requisiti di cui al paragrafo 4 in merito ai propri piani nazionali di risposta agli incidenti e delle crisi di cibersicurezza su vasta scala entro tre mesi dall'adozione di tali piani. Gli Stati membri possono omettere informazioni se e nella misura in cui ciò sia necessario ai fini della loro sicurezza nazionale.	
Articolo 10 **Team di risposta agli incidenti di sicurezza informatica (CSIRT)** 1. Ogni Stato membro designa o istituisce uno o più CSIRT. È possibile designare o istituire i CSIRT all'interno di un'autorità competente. I CSIRT sono conformi ai requisiti di cui all'articolo 11, paragrafo 1, si occupano almeno dei settori, dei sottosettori e dei tipi di soggetto di cui agli allegati I e II e sono responsabili della gestione degli incidenti conformemente a una procedura ben definita. 2. Gli Stati membri provvedono affinché ogni CSIRT disponga di risorse adeguate per svolgere efficacemente i suoi compiti di cui all'articolo 11, paragrafo 3. 3. Gli Stati membri provvedono affinché ogni CSIRT disponga di un'infrastruttura di informazione e comunicazione adeguata, sicura e resiliente attraverso la quale scambiare	**ART. 15** ***(Gruppo nazionale di risposta agli incidenti di sicurezza informatica – CSIRT Italia)***

informazioni con i soggetti essenziali e importanti e con gli altri portatori di interesse pertinenti. A tal fine gli Stati membri provvedono affinché ogni CSIRT contribuisca allo sviluppo di strumenti sicuri per la condivisione delle informazioni. 4. I CSIRT cooperano e, se opportuno, scambiano informazioni pertinenti conformemente all'articolo 29 con comunità settoriali o intersettoriali di soggetti essenziali e importanti. 5. I CSIRT partecipano alle revisioni tra pari organizzate conformemente all'articolo 19. 6. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro CSIRT nella rete di CSIRT. 7. I CSIRT possono stabilire relazioni di cooperazione con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi. Nell'ambito di tali relazioni di cooperazione, gli Stati membri facilitano uno scambio di informazioni efficace, efficiente e sicuro con tali team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, utilizzando i pertinenti protocolli di condivisione delle informazioni, compreso il protocollo TLP (Traffic Light Protocol). I CSIRT possono scambiare informazioni pertinenti con team nazionali di risposta agli incidenti di sicurezza informatica di paesi terzi, compresi dati personali a norma del diritto dell'Unione in materia di protezione dei dati. 8. I CSIRT possono cooperare con team 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 cibersicurezza. 9. Ogni Stato membro notifica alla Commissione senza indebiti ritardi l'identità del CSIRT di cui al paragrafo 1 del presente articolo e del CSIRT designato come coordinatore conformemente all'articolo 12, paragrafo 1, i rispettivi compiti in relazione ai soggetti essenziali e importanti e qualsiasi ulteriore modifica dei medesimi. 10. Gli Stati membri possono chiedere l'assistenza dell'ENISA nello sviluppo dei CSIRT.	

Articolo 11 **Requisiti, capacità tecniche e compiti dei CSIRT**	**ART. 15** ***(Gruppo nazionale di risposta agli incidenti di sicurezza informatica – CSIRT Italia)***
1. I CSIRT soddisfano i requisiti seguenti:	
a) i CSIRT garantiscono un alto livello di disponibilità dei propri canali di comunicazione evitando singoli punti di vulnerabilità (single points of failure) e dispongono di vari mezzi che permettono loro di essere contattati e di contattare altri in qualsiasi momento; essi indicano chiaramente i canali di comunicazione e li rendono noti alla loro base di utenti e ai partner con cui collaborano;	
b) i locali e i sistemi informatici di supporto dei CSIRT sono ubicati in siti sicuri;	
c) i CSIRT sono dotati di un sistema adeguato di gestione e inoltro delle richieste, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;	
d) i CSIRT garantiscono la riservatezza e l'affidabilità delle loro operazioni;	
e) i CSIRT dispongono di personale sufficiente per garantire la disponibilità dei loro servizi in qualsiasi momento e garantiscono che il loro personale sia formato in modo appropriato;	
f) i CSIRT sono dotati di sistemi ridondanti e spazi di lavoro di backup al fine di garantire la continuità dei loro servizi.	
I CSIRT hanno la possibilità di partecipare a reti di cooperazione internazionale.	
2. Gli Stati membri assicurano che i loro CSIRT dispongano congiuntamente delle capacità tecniche necessarie a svolgere i compiti di cui al paragrafo 3. Gli Stati membri provvedono affinché ai propri CSIRT siano assegnate risorse sufficienti per garantire un organico adeguato al fine di consentire ai CSIRT di sviluppare le proprie capacità tecniche.	
3. I CSIRT svolgono i compiti seguenti:	
a) monitorano e analizzano le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale, e, su richiesta, forniscono assistenza ai soggetti essenziali e importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informatici e di rete;	
b) emettono preallarmi, allerte e bollettini e divulgano informazioni ai soggetti essenziali e	

importanti interessati, nonché alle autorità competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale; c) forniscono una risposta agli incidenti e forniscono assistenza ai soggetti essenziali e importanti interessati, se del caso; d) raccolgono e analizzano dati forensi e forniscono un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla cibersicurezza; e) effettuano, su richiesta di un soggetto essenziale o importante, una scansione proattiva dei sistemi informatici e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo; f) partecipano alla rete di CSIRT e forniscono assistenza reciproca secondo le loro capacità e competenze agli altri membri della rete di CSIRT su loro richiesta. g) se del caso, agiscono in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1; h) contribuiscono allo sviluppo di strumenti sicuri per la condivisione delle informazioni di cui all'articolo 10, paragrafo 3. I CSIRT possono effettuare una scansione proattiva e non intrusiva dei sistemi informatici e di rete accessibili al pubblico di soggetti essenziali e importanti. Tale scansione è effettuata per individuare sistemi informatici 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. Nello svolgimento dei compiti di cui al primo comma, i CSIRT possono dare priorità a determinati compiti sulla base di un approccio basato sul rischio. 4. I CSIRT instaurano rapporti di cooperazione con i pertinenti portatori di interesse del settore privato al fine di perseguire gli obiettivi della presente direttiva. 5. Al fine di agevolare la cooperazione di cui al paragrafo 4, i CSIRT promuovono l'adozione e l'uso di pratiche, sistemi di classificazione e	

tassonomie standardizzati o comuni per quanto riguarda: a) le procedure di gestione degli incidenti; b) la gestione delle crisi; e c) la divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12, paragrafo 1.	
Articolo 12 **Divulgazione coordinata delle vulnerabilità e banca dati europea delle vulnerabilità** 1. Ogni Stato membro designa uno dei propri CSIRT come coordinatore ai fini della divulgazione coordinata delle vulnerabilità. Il CSIRT designato agisce da intermediario di fiducia agevolando, se necessario, l'interazione 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. I compiti del CSIRT designato come coordinatore comprendono: a) l'individuazione e il contatto dei soggetti interessati; b) l'assistenza alle persone fisiche o giuridiche che segnalano una vulnerabilità, e c) la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità che interessano più soggetti. Gli Stati membri provvedono affinché le persone fisiche o giuridiche possano segnalare in forma anonima, qualora lo richiedano, una vulnerabilità al CSIRT designato come coordinatore. Il CSIRT designato come coordinatore garantisce lo svolgimento di diligenti azioni per dare seguito alla segnalazione di vulnerabilità e assicura l'anonimato della persona fisica o giuridica segnalante. Se la vulnerabilità segnalata è suscettibile di avere un impatto significativo su soggetti in più di uno Stato membro, il CSIRT designato di ciascuno Stato membro interessato coopera, se del caso, con altri CSIRT designati in qualità di coordinatori nell'ambito della rete di CSIRT. 2. L'ENISA elabora e mantiene, previa consultazione del gruppo di cooperazione, una banca dati europea delle vulnerabilità. A tal fine	**ART. 16** ***(Divulgazione coordinata delle vulnerabilità)***

l'ENISA istituisce e gestisce i sistemi informatici, le misure strategiche e le procedure adeguati e adotta le necessarie misure tecniche e organizzative per garantire la sicurezza e l'integrità della banca dati europea delle vulnerabilità, in particolare al fine di consentire ai soggetti, indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione della presente direttiva, e ai relativi fornitori di sistemi informatici e di rete, di divulgare e registrare, su base volontaria, le vulnerabilità pubblicamente note presenti nei prodotti TIC o nei servizi TIC. Tutti i portatori di interessi hanno accesso alle informazioni sulle vulnerabilità contenute nella banca dati europea delle vulnerabilità. La banca dati contiene: a) informazioni che illustrano la vulnerabilità; b) i prodotti TIC o i servizi TIC interessati e la gravità della vulnerabilità in termini di circostanze nelle quali potrebbe essere sfruttata; 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 derivanti dalle vulnerabilità divulgate.	
Articolo 13 **Cooperazione a livello nazionale** 1. Se sono separati, le autorità competenti, il punto di contatto unico e i CSIRT dello stesso Stato membro collaborano per quanto concerne l'adempimento degli obblighi di cui alla presente direttiva. 2. Gli Stati membri provvedono affinché i loro CSIRT o, se del caso, le loro autorità competenti, ricevano le notifiche degli incidenti significativi a norma dell'articolo 23, nonché degli incidenti, delle minacce informatiche e dei quasi incidenti (near miss) a norma dell'articolo 30. 3. Gli Stati membri provvedono affinché i loro CSIRT o, se del caso, le loro autorità competenti informino i loro punti di contatto unico delle notifiche relative agli incidenti, alle minacce informatiche e ai quasi incidenti trasmesse a norma della presente direttiva.	**ART. 14** ***(Cooperazione tra Autorità nazionali)***

4. Al fine di garantire l'efficace adempimento dei compiti e degli obblighi delle autorità competenti, dei punti di contatto unici e dei CSIRT, gli Stati membri, nella misura del possibile, provvedono affinché, all'interno di ciascuno Stato membro, vi sia un'adeguata cooperazione tra i suddetti organismi e le autorità di contrasto, le autorità di protezione dei dati, le autorità nazionali ai sensi dei regolamenti (CE) n. 300/2008 e (UE) 2018/1139, gli organismi di vigilanza a norma del regolamento (UE) n. 910/2014, le autorità competenti a norma del regolamento (UE) 2022/2554, le autorità nazionali di regolamentazione a norma della direttiva (UE) 2018/1972, le autorità competenti a norma della direttiva (UE) 2022/2557, nonché le autorità competenti ai sensi di altri atti giuridici settoriali dell'Unione. 5. Gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva e le loro autorità competenti a norma della direttiva (UE) 2022/2557 collaborino e si scambino periodicamente informazioni riguardo all'identificazione di soggetti critici, sui rischi, sulle minacce e sugli incidenti sia informatici che non informatici che interessano i soggetti essenziali identificati come critici a norma della direttiva (UE) 2022/2557, e sulle misure adottate in risposta a tali rischi, minacce e incidenti. Gli Stati membri provvedono inoltre affinché le loro autorità competenti a norma della presente direttiva e le loro autorità competenti a norma del regolamento (UE) n. 910/2014, del regolamento (UE) 2022/2554 e della direttiva (UE) 2018/1972 si scambino periodicamente informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti. 6. Gli Stati membri semplificano la comunicazione mediante i mezzi tecnici per le notifiche di cui agli articoli 23 e 30.	
CAPO III **COOPERAZIONE A LIVELLO DELL'UNIONE E INTERNAZIONALE**	
Articolo 14 **Gruppo di cooperazione**	**ART. 18** ***(Gruppo di cooperazione NIS)***

1. Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri, nonché di rafforzare la fiducia, è istituito un gruppo di cooperazione. 2. Il gruppo di cooperazione svolge i suoi compiti sulla base di programmi di lavoro biennali di cui al paragrafo 7. 3. Il gruppo di cooperazione è composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA. Il Servizio europeo per l'azione esterna partecipa alle attività del gruppo di cooperazione in qualità di osservatore. Le autorità europee di vigilanza (AEV) e le autorità competenti a norma del regolamento (UE) 2022/2554 possono partecipare alle attività del gruppo di cooperazione conformemente all'articolo 47, paragrafo 1, di tale regolamento. Ove opportuno, il gruppo di cooperazione può invitare a partecipare ai suoi lavori il Parlamento europeo e i rappresentanti dei pertinenti portatori di interessi. La Commissione ne assicura il segretariato. 4. Il gruppo di cooperazione svolge i compiti seguenti: a) fornire orientamenti alle autorità competenti in merito al recepimento e all'attuazione della presente direttiva; b) fornire orientamenti alle autorità competenti in merito allo sviluppo e all'attuazione di politiche in materia di divulgazione coordinata delle vulnerabilità di cui all'articolo 7, paragrafo 2, lettera c); c) scambiare migliori prassi e informazioni relative all'attuazione della presente direttiva, anche per quanto riguarda minacce informatiche, incidenti, vulnerabilità, quasi incidenti, iniziative di sensibilizzazione, attività di formazione, esercitazioni e competenze, sviluppo di capacità, norme e specifiche tecniche, nonché l'identificazione dei soggetti essenziali e importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e); d) effettuare scambi di consulenza e cooperare con la Commissione per quanto riguarda le nuove iniziative strategiche in materia di cibersicurezza e la coerenza globale dei requisiti settoriali di cibersicurezza;	

e) effettuare scambi di consulenza e cooperare con la Commissione per quanto riguarda i progetti di atti delegati o di esecuzione adottati a norma della presente direttiva; f) scambiare migliori prassi e informazioni con le istituzioni, gli organismi, gli uffici e le agenzie pertinenti dell'Unione; g) effettuare scambi di opinioni per quanto riguarda l'attuazione degli atti giuridici settoriali dell'Unione che contengono disposizioni in materia di cibersicurezza; h) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9 ed elaborare conclusioni e raccomandazioni; i) effettuare valutazioni coordinate dei rischi per la sicurezza di catene di approvvigionamento critiche conformemente all'articolo 22, paragrafo 1; j) discutere i casi di assistenza reciproca, fra cui le esperienze e i risultati delle azioni di vigilanza comuni transfrontaliere di cui all'articolo 37; k) su richiesta di uno o più Stati membri interessati, discutere le richieste specifiche di assistenza reciproca di cui all'articolo 37; l) fornire orientamenti strategici alla rete di CSIRT ed EU–CyCLONe su specifiche questioni emergenti; m) effettuare scambi di opinioni sulla politica in materia di azioni di follow-up a seguito incidenti e crisi di cibersicurezza su vasta scala sulla base degli insegnamenti tratti dalla rete di CSIRT e da EU-CyCLONe; n) contribuire alle capacità di cibersicurezza in tutta l'Unione agevolando lo scambio di funzionari nazionali attraverso un programma di sviluppo delle capacità che coinvolga il personale delle autorità competenti o dei CSIRT; o) organizzare riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato di tutta l'Unione per discutere le attività svolte dal gruppo di cooperazione e raccogliere contributi sulle sfide strategiche emergenti; p) discutere le attività intraprese per quanto riguarda le esercitazioni di cibersicurezza, compreso il lavoro svolto dall'ENISA; q) stabilire la metodologia e gli aspetti organizzativi delle revisioni tra pari di cui all'articolo 19, paragrafo 1, nonché stabilire, con	

l'assistenza della Commissione e dell'ENISA, la metodologia di autovalutazione per gli Stati membri a norma dell'articolo 19, paragrafo 4, ed elaborare, in collaborazione con la Commissione e l'ENISA, i codici di condotta su cui si basano i metodi di lavoro degli esperti di cibersicurezza designati a norma dell'articolo 19, paragrafo 6; r) elaborare relazioni, ai fini del riesame di cui all'articolo 40, sull'esperienza acquisita a livello strategico e dalle revisioni tra pari; s) discutere e svolgere periodicamente una valutazione dello stato di avanzamento delle minacce o degli incidenti informatici, come il ransomware. Il gruppo di cooperazione presenta le relazioni di cui al primo comma, lettera r), alla Commissione, al Parlamento europeo e al Consiglio. 5. Gli Stati membri garantiscono la collaborazione effettiva, efficiente e sicura dei loro rappresentanti in seno al gruppo di cooperazione. 6. Il gruppo di cooperazione può richiedere alla rete di CSIRT una relazione tecnica su argomenti selezionati. 7. Entro il 1o febbraio 2024e successivamente ogni due anni, il gruppo di cooperazione stabilisce un programma di lavoro sulle azioni da intraprendere per realizzare i propri obiettivi e compiti. 8. La Commissione può adottare atti di esecuzione che stabiliscono le modalità procedurali necessarie per il funzionamento del gruppo di cooperazione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2. La Commissione scambia pareri e coopera con il gruppo di cooperazione in merito ai progetti di atto di esecuzione di cui al primo comma del presente paragrafo, conformemente al paragrafo 4, lettera e). 9. Il gruppo di cooperazione si riunisce periodicamente, e in ogni caso una volta all'anno, con il gruppo per la resilienza dei soggetti critici istituito a norma della direttiva (UE) 2022/2557 al fine di promuovere e	

agevolare la cooperazione strategica e lo scambio di informazioni.	
Articolo 15 **Rete di CSIRT** 1. Al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri, è istituita una rete dei CSIRT nazionali. 2. La rete di CSIRT è composta da rappresentanti dei CSIRT designati o istituiti a norma dell'articolo 10 e della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'Unione (CERT-UE). La Commissione partecipa alla rete di CSIRT in qualità di osservatore. L'ENISA ne assicura il segretariato e fornisce attivamente assistenza alla cooperazione fra i CSIRT. 3. La rete di CSIRT svolge i compiti seguenti: a) scambiare informazioni per quanto riguarda le capacità dei CSIRT; b) agevolare 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; c) scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità; d) scambiare informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di cibersicurezza; 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 potenzialmente interessato da un incidente, scambiare e discutere informazioni relative a tale incidente e alle minacce informatiche, ai rischi e alle vulnerabilità associati; g) su richiesta di un membro della rete di CSIRT, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro; h) fornire assistenza agli Stati membri nel far fronte a incidenti transfrontalieri a norma della presente direttiva; i) cooperare e scambiare migliori pratiche con i CSIRT designati in qualità di coordinatori di cui	**ART. 20** ***(Rete di CSIRT nazionali)***

all'articolo 12, paragrafo 1, 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; j) discutere e individuare ulteriori forme di cooperazione operativa, anche in relazione a: i) categorie di minacce informatiche e incidenti; ii) preallarmi; iii) assistenza reciproca; iv) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri; v) contributi al piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4, su richiesta di uno Stato membro; k) informare il gruppo di cooperazione sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera j) e, se necessario, chiedere orientamenti in merito; l) fare il punto sui risultati delle esercitazioni di cibersicurezza, comprese quelle organizzate dall'ENISA; m) su richiesta di un singolo CSIRT, discutere le capacità e lo stato di preparazione di tale CSIRT; n) cooperare e scambiare informazioni con i centri operativi di sicurezza regionali e a livello dell'UE al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche in tutta l'Unione; o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9; p) fornire orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa. 4. Entro il 17 gennaio 2025, e successivamente ogni due anni, ai fini del riesame di cui all'articolo 40, la rete di CSIRT valuta i progressi compiuti nella cooperazione operativa ed elabora una relazione. Nella relazione, in particolare, vengono elaborate conclusioni e raccomandazioni sulla base del risultato delle revisioni tra pari di cui all'articolo 19, che sono	

effettuate in relazione ai CSIRT nazionali. Tale relazione è trasmessa al gruppo di cooperazione. 5. La rete di CSIRT adotta il proprio regolamento interno. 6. La rete di CSIRT ed EU-CyCLONe concordano le modalità procedurali e cooperano su tale base.	
Articolo 16 **Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)** 1. EU-CyCLONe è istituita al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. 2. EU-CyCLONe è composta da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri e, nei casi in cui un incidente di cibersicurezza su vasta scala potenziale o in corso abbia o abbia probabilità di avere un impatto significativo sui servizi e sulle attività che rientrano nell'ambito di applicazione della presente direttiva, della Commissione. Negli altri casi, la Commissione partecipa alle attività di EU-CyCLONe in qualità di osservatore. L'ENISA assicura il segretariato di EU-CyCLONe e sostiene lo scambio sicuro di informazioni, oltre a fornire gli strumenti necessari per sostenere la cooperazione tra gli Stati membri garantendo uno scambio sicuro di informazioni. Ove opportuno, EU-CyCLONe può invitare i rappresentanti dei pertinenti portatori di interessi a partecipare ai suoi lavori in qualità di osservatori. 3. EU-CyCLONe svolge i compiti seguenti: a) aumentare il livello di preparazione per la gestione di crisi e incidenti su vasta scala; b) sviluppare una conoscenza situazionale condivisa in merito agli incidenti e alle crisi di cibersicurezza su vasta scala; c) valutare le conseguenze e l'impatto dei pertinenti incidenti e delle pertinenti crisi di cibersicurezza su vasta scala e proporre possibili misure di attenuazione;	**ART. 19** ***(Rete delle organizzazioni di collegamento per le crisi informatiche - EU-CyCLONe)***

d) coordinare la gestione degli incidenti e delle crisi di cibersicurezza su vasta scala e sostenere il processo decisionale a livello politico in merito a tali incidenti e crisi; e) discutere, su richiesta di uno Stato membro interessato, i piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4. 4. EU-CyCLONe adotta il proprio regolamento interno. 5. EU-CyCLONe riferisce periodicamente al gruppo di cooperazione in merito alla gestione degli incidenti e delle crisi di cibersicurezza su vasta scala, nonché in merito alle tendenze, concentrandosi in particolare sul relativo impatto sui soggetti essenziali e importanti. 6. EU-CyCLONe coopera con la rete di CSIRT sulla base di modalità procedurali concordate previste all'articolo 15, paragrafo 6. 7. Entro il 17 luglio 2024e successivamente ogni 18 mesi, EU-CyCLONe presenta al Parlamento europeo e al Consiglio una relazione di valutazione del proprio lavoro.	
Articolo 17 **Cooperazione internazionale** Ove opportuno, l'Unione può concludere accordi internazionali, conformemente all'articolo 218 TFUE, con paesi terzi o organizzazioni internazionali, che consentano e organizzino la loro partecipazione ad attività particolari del gruppo di cooperazione, della rete di CSIRT e di EU-CyCLONe. Tali accordi sono conformi al diritto dell'Unione in materia di protezione dei dati.	*Non richiede recepimento.*
Articolo 18 **Relazione sullo stato della cibersicurezza nell'Unione** 1. L'ENISA, in collaborazione con la Commissione e con il gruppo di cooperazione, pubblica una relazione biennale sullo stato della cibersicurezza nell'Unione e la presenta al Parlamento europeo. La relazione è resa disponibile, fra l'altro, in un formato leggibile meccanicamente e comprende gli aspetti seguenti:	*Non richiede recepimento.*

a) una valutazione del rischio di cibersicurezza a livello dell'Unione, che tenga conto del panorama delle minacce informatiche; b) una valutazione dello sviluppo delle capacità di cibersicurezza nei settori pubblico e privato nell'Unione; c) una valutazione del livello generale di consapevolezza in materia di cibersicurezza e di igiene informatica tra i cittadini e i soggetti, comprese le piccole e medie imprese; d) una valutazione aggregata del risultato delle revisioni tra pari di cui all'articolo 19; e) una valutazione aggregata del livello di maturità delle capacità e delle risorse di cibersicurezza nell'Unione, comprese quelle a livello settoriale, nonché del livello di allineamento delle strategie nazionali di cibersicurezza degli Stati membri. 2. La relazione contiene raccomandazioni strategiche specifiche, finalizzate a porre rimedio alle carenze e ad aumentare il livello di cibersicurezza nell'Unione, e una sintesi delle conclusioni tratte per quel determinato periodo nelle relazioni sulla situazione tecnica della cibersicurezza nell'Unione per quanto riguarda gli incidenti e le minacce informatiche, elaborate dall'ENISA conformemente all'articolo 7, paragrafo 6, del regolamento (UE) 2019/881. 3. L'ENISA, in collaborazione con la Commissione, il gruppo di cooperazione e la rete di CSIRT, elabora la metodologia, ivi comprese le variabili pertinenti — come ad esempio indicatori quantitativi e qualitativi — della valutazione aggregata di cui al paragrafo 1, lettera e).	
Articolo 19 **Revisioni tra pari** 1. Con l'assistenza della Commissione e dell'ENISA nonché, se del caso, della rete CSIRT ed entro il 17 gennaio 2025, il gruppo di cooperazione stabilisce la metodologia e gli aspetti organizzativi delle revisioni tra pari con 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 presente direttiva. La partecipazione alle revisioni tra pari è volontaria. Le revisioni tra pari sono condotte da	**ART. 21** ***(Procedura di revisione tra pari)***

esperti di cibersicurezza. Gli esperti di cibersicurezza sono designati da almeno due Stati membri, diversi dallo Stato membro oggetto di revisione. Le revisioni tra pari riguardano almeno uno degli aspetti seguenti: a) il livello di attuazione delle misure di gestione e delle prescrizioni in materia di segnalazione dei rischi di cibersicurezza enunciate agli articoli 21 e 23; b) il livello delle capacità, comprese le risorse finanziarie, tecniche e umane disponibili, e l'efficacia dello svolgimento dei compiti delle autorità competenti; c) le capacità operative dei CSIRT; d) il livello di attuazione dell'assistenza reciproca di cui all'articolo 37; e) il livello di attuazione degli accordi per la condivisione delle informazioni in materia di cibersicurezza di cui all'articolo 29; f) le questioni specifiche di natura transfrontaliera o intersettoriale. 2. La metodologia di cui al paragrafo 1 comprende criteri obiettivi, non discriminatori, equi e trasparenti sulla base dei quali gli Stati membri designano esperti di cibersicurezza idonei a eseguire le revisioni tra pari. La Commissione e l'ENISA partecipano alle revisioni tra pari in qualità di osservatori. 3. Gli Stati membri possono individuare questioni specifiche di cui al paragrafo 1, lettera f), ai fini di una revisione tra pari. 4. Prima dell'inizio di una revisione tra pari di cui al paragrafo 1, gli Stati membri notificano agli Stati membri partecipanti il suo ambito di applicazione, comprese le questioni specifiche individuate ai sensi del paragrafo 3. 5. Prima dell'inizio della revisione tra pari, gli Stati membri possono effettuare un'autovalutazione degli aspetti oggetto della revisione e fornire tale autovalutazione agli esperti di cibersicurezza designati. Il gruppo di cooperazione, con l'assistenza della Commissione e dell'ENISA, stabilisce la metodologia per l'autovalutazione degli Stati membri. 6. Le revisioni tra pari comportano visite in loco fisiche o virtuali e scambi di informazioni a	

distanza. In linea con il principio di buona collaborazione, lo Stato membro sottoposto alla revisione tra pari fornisce agli esperti di cibersicurezza designati le informazioni necessarie per la valutazione, fatta salva la legislazione nazionale o dell'Unione in materia di protezione di informazioni riservate o classificate e di salvaguardia delle funzioni essenziali dello Stato, quali la sicurezza nazionale. Il gruppo di cooperazione, in collaborazione con la Commissione e con l'ENISA, elabora codici di condotta adeguati, su cui si basano i metodi di lavoro degli esperti di cibersicurezza designati. Le informazioni ottenute mediante la revisione tra pari sono utilizzate unicamente a tal fine. Gli esperti di cibersicurezza che partecipano alla revisione tra pari non divulgano a terzi le eventuali informazioni sensibili o riservate ottenute nel corso di tale revisione tra pari. 7. Una volta sottoposti a revisione tra pari, i medesimi aspetti esaminati in uno Stato membro non sono più soggetti a ulteriori revisioni tra pari in tale Stato membro per i due anni successivi alla conclusione della revisione, a meno che non sia diversamente richiesto o stabilito dallo Stato membro su proposta del gruppo di cooperazione. 8. Gli Stati membri provvedono affinché gli eventuali rischi di conflitto di interessi riguardanti gli esperti di cibersicurezza designati siano rivelati agli altri Stati membri, al gruppo di cooperazione, alla Commissione e all'ENISA prima dell'inizio della revisione tra pari. Lo Stato membro che è sottoposto alla revisione tra pari può opporsi alla designazione di particolari esperti di cibersicurezza per motivi debitamente giustificati, comunicati allo Stato membro designante. 9. Gli esperti di cibersicurezza che partecipano alle revisioni tra pari elaborano relazioni sui risultati e sulle conclusioni delle revisioni tra pari. Gli Stati membri sottoposti a revisione tra pari possono formulare osservazioni sui progetti di relazione che li riguardano e tali osservazioni sono allegate alle relazioni. Le relazioni contengono raccomandazioni che consentono di migliorare gli aspetti sottoposti alla revisione tra pari. Le relazioni sono presentate al gruppo di cooperazione e alla rete di CSIRT, se del caso.	

Uno Stato membro sottoposto alla revisione tra pari può decidere di rendere pubblica la sua relazione o una sua versione espunta.	
CAPO IV **MISURE DI GESTIONE DEL RISCHIO DI CIBERSICUREZZA E OBBLIGHI DI SEGNALAZIONE**	
Articolo 20 **Governance** 1. 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 per conformarsi all'articolo 21, sovraintendano alla sua attuazione e possano essere ritenuti responsabili di violazione da parte dei soggetti di tale articolo. L'applicazione del presente paragrafo lascia impregiudicato il diritto nazionale per quanto riguarda le norme in materia di responsabilità applicabili alle istituzioni pubbliche, nonché la responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati. 2. Gli Stati membri provvedono affinché i membri dell'organo di gestione dei soggetti essenziali e importanti siano tenuti a seguire una formazione e incoraggiano i soggetti essenziali e importanti a offrire periodicamente una formazione analoga ai loro dipendenti, per far sì che questi acquisiscano conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi di cibersicurezza e il loro impatto sui servizi offerti dal soggetto.	**ART. 23** ***(Organi di amministrazione e direttivi)*** Confronta anche: **- ART. 31 (*Proporzionalità e gradualità degli obblighi*)** **- ART. 32 *(Previsioni settoriali specifiche)***
Articolo 21 **Misure di gestione dei rischi di cibersicurezza** 1. Gli Stati membri provvedono 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 o nella fornitura dei loro servizi, nonché per prevenire	**ART. 24** ***(Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica)*** Confronta anche: **- ART. 30 *(Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi)*** **- ART. 31 (*Proporzionalità e gradualità degli obblighi*)**

o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, le misure di cui al primo comma assicurano un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. Nel valutare la proporzionalità di tali misure, si tiene debitamente conto del grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico. 2. Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti: a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici; b) gestione degli incidenti; c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi; d) sicurezza della catena di approvvigionamento, compresi 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 informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità; f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza; g) pratiche di igiene informatica di base e formazione in materia di cibersicurezza; h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura; i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi; j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di	**- ART. 32** ***(Previsioni settoriali specifiche)***

comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso. 3. Gli Stati membri provvedono affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), del presente articolo, siano adeguate, i soggetti tengano conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di cibersicurezza dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Gli Stati membri provvedono inoltre affinché, nel valutare quali misure di cui al paragrafo 2, lettera d), siano adeguate, i soggetti siano tenuti a tenere conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate a norma dell'articolo 22, paragrafo 1. 4. Gli Stati membri provvedono affinché, qualora un soggetto constati di non essere conforme alle misure di cui al paragrafo 2, esso adotti, senza indebito ritardo, tutte le misure correttive necessarie, appropriate e proporzionate. 5. Entro il 17 ottobre 2024, la Commissione adotta atti di esecuzione che stabiliscono i requisiti tecnici e metodologici delle misure di cui al paragrafo 2 per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, 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, nonché i prestatori di servizi fiduciari. La Commissione può adottare atti di esecuzione che stabiliscono i requisiti tecnici e metodologici, nonché, se necessario, i requisiti settoriali relativi alle misure di cui al paragrafo 2 per quanto riguarda i soggetti essenziali e importanti diversi da quelli di cui al primo comma del presente paragrafo. Nell'elaborare gli atti di esecuzione di cui al primo e secondo comma del presente paragrafo, la Commissione segue, nella misura del possibile, le norme europee e internazionali, nonché le pertinenti specifiche tecniche. La Commissione scambia pareri e coopera con il	

gruppo di cooperazione e con l'ENISA in merito ai progetti di atto di esecuzione conformemente all'articolo 14, paragrafo 4, lettera e). Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.	
Articolo 22 **Valutazioni coordinate a livello dell'Unione del rischio per la sicurezza delle catene di approvvigionamento critiche** 1. Il gruppo di cooperazione, in collaborazione con la Commissione e l'ENISA, può effettuare valutazioni coordinate dei rischi per la sicurezza di specifiche catene di approvvigionamento critiche di servizi TIC, sistemi TIC o prodotti TIC, tenendo conto dei fattori di rischio tecnici e, se opportuno, non tecnici. 2. La Commissione, previa consultazione del gruppo di cooperazione e dell'ENISA, nonché, ove necessario, dei pertinenti portatori di interessi, identifica i servizi TIC, i sistemi TIC o i prodotti TIC critici specifici che possono essere oggetto della valutazione coordinata del rischio per la sicurezza di cui al paragrafo 1.	
Articolo 23 **Obblighi di segnalazione** 1. Ciascuno Stato membro provvede affinché i soggetti essenziali e importanti notifichino senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, conformemente al paragrafo 4, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi quali indicati al paragrafo 3 (incidente significativo). Se opportuno, i soggetti interessati notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi. Ciascuno Stato membro provvede affinché tali soggetti comunichino, tra l'altro, qualunque informazione che consenta al CSIRT o, se opportuno, all'autorità competente di determinare l'eventuale impatto transfrontaliero dell'incidente. La sola notifica non espone il soggetto che la effettua a una maggiore responsabilità. Qualora i soggetti interessati notifichino all'autorità competente un incidente significativo conformemente al primo comma, lo Stato membro provvede affinché l'autorità	**ART. 25** ***(Obblighi in materia di notifica di incidente)*** **- ART. 31 (*Proporzionalità e gradualità degli obblighi*)** **- ART. 32 *(Previsioni settoriali specifiche)***

competente inoltri la notifica al CSIRT dopo averla ricevuta. In caso di incidente significativo transfrontaliero o intersettoriale, gli Stati membri provvedono affinché i loro punti di contatto unici ricevano in tempo utile informazioni pertinenti notificate conformemente al paragrafo 4. 3. Un incidente è considerato significativo se: a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli. 2. Se opportuno, gli Stati membri provvedono affinché i soggetti essenziali e importanti comunichino senza indebito ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa qualsiasi misura o azione correttiva che tali destinatari sono in grado di adottare in risposta a tale minaccia. Se opportuno, i soggetti informano tali destinatari anche della minaccia informatica significativa stessa. 4. Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente: a) senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero; b) senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, 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; c) su richiesta di un CSIRT o, se opportuno, di un'autorità competente, 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: i) una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto; ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente; iii) le misure di attenuazione adottate e in corso; iv) se opportuno, l'impatto transfrontaliero dell'incidente; e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), gli Stati membri provvedono affinché i soggetti interessati forniscano una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente. In deroga al primo comma, lettera b), un prestatore di servizi fiduciari, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, informa il CSIRT o, se opportuno, l'autorità competente senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo. 5. Senza indebito ritardo e ove possibile entro 24 ore dal ricevimento del preallarme di cui al paragrafo 4, lettera a), il CSIRT o l'autorità competente fornisce una risposta al soggetto notificante, comprendente un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza operativa sull'attuazione di possibili misure di attenuazione. Se il CSIRT non è il destinatario iniziale della notifica di cui al paragrafo 1, gli orientamenti sono forniti dall'autorità competente in cooperazione con il CSIRT. Su richiesta del soggetto interessato, il CSIRT fornisce ulteriore supporto tecnico. Qualora si sospetti che l'incidente significativo abbia carattere criminale, il CSIRT o l'autorità competente fornisce anche orientamenti sulla segnalazione dell'incidente significativo alle autorità di contrasto. 6. Se opportuno, e in particolare se l'incidente significativo interessa due o più Stati membri, il CSIRT, l'autorità competente o il punto di contatto unico ne informa senza indebito ritardo	

gli altri Stati membri interessati e l'ENISA. Tali informazioni includono o il tipo di informazioni ricevute a norma del paragrafo 4. Nel fare ciò, il CSIRT, l'autorità competente o il punto di contatto unico tutelano, in conformità al diritto dell'Unione o nazionale, la sicurezza e gli interessi commerciali del soggetto nonché la riservatezza delle informazioni fornite. 7. Qualora sia necessario sensibilizzare il pubblico per evitare un incidente significativo o affrontare un incidente significativo in corso, o qualora la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico, dopo aver consultato il soggetto interessato il CSIRT di uno Stato membro o, se del caso, la sua autorità competente e, se opportuno, i CSIRT o le autorità competenti degli altri Stati membri interessati, possono informare il pubblico riguardo all'incidente significativo o imporre al soggetto di farlo. 8. Su richiesta del CSIRT o dell'autorità competente, il punto di contatto unico inoltra le notifiche ricevute a norma del paragrafo 1 ai punti di contatto unici degli altri Stati membri interessati. 9. Il punto di contatto unico trasmette ogni tre mesi all'ENISA una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi incidenti notificati conformemente al paragrafo 1 del presente articolo e all'articolo 30. Al fine di contribuire alla fornitura di informazioni comparabili, l'ENISA può adottare orientamenti tecnici sui parametri delle informazioni da includere nella relazione di sintesi. Ogni sei mesi l'ENISA informa il gruppo di cooperazione e la rete di CSIRT delle sue constatazioni in merito alle notifiche ricevute. 10. I CRSIRT o, se opportuno, le autorità competenti forniscono alle autorità competenti a norma della direttiva (UE) 2022/2557 le informazioni sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi incidenti notificati conformemente al paragrafo 1 del presente articolo e all'articolo 30 dai soggetti identificati come soggetti critici a norma della direttiva (UE) 2022/2557. 11. La Commissione può adottare atti di esecuzione che specifichino ulteriormente il tipo	

di informazioni, il relativo formato e la procedura di trasmissione di una notifica a norma del paragrafo 1 del presente articolo e dell'articolo 30 e di una comunicazione trasmessa a norma del paragrafo 2 del presente articolo. Entro il 17 ottobre 2024 la Commissione adotta, per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, 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, nonché 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, atti di esecuzione che specifichino ulteriormente i casi in cui un incidente debba essere considerato significativo come indicato al paragrafo 3. La Commissione può adottare tali atti di esecuzione in relazione ad altri soggetti essenziali e importanti. La Commissione scambia pareri e coopera con il gruppo di cooperazione in merito ai progetti di atto di esecuzione di cui al primo e secondo comma del presente paragrafo conformemente all'articolo 14, paragrafo 4, lettera e). Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 39, paragrafo 2.	
Articolo 24 **Uso dei sistemi europei di certificazione della cibersicurezza** 1. Al fine di dimostrare il rispetto di determinate prescrizioni di cui all'articolo 21, gli Stati membri possono imporre ai soggetti essenziali e importanti di utilizzare determinati prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito dei sistemi europei di certificazione della cibersicurezza adottati a norma dell'articolo 49 del regolamento (UE) 2019/881. Inoltre, gli Stati membri incoraggiano i soggetti essenziali e importanti a utilizzare servizi fiduciari qualificati. 2. Alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 38 al	**ART. 27** ***(Uso di schemi di certificazione della cybersicurezza)*** Confronta anche: **- ART. 31 (*Proporzionalità e gradualità degli obblighi*)** **- ART. 32 *(Previsioni settoriali specifiche)***

fine di integrare la presente direttiva specificando quali categorie di soggetti essenziali e importanti sono tenute a utilizzare determinati prodotti TIC, servizi TIC e processi TIC certificati o a ottenere un certificato nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 49 del regolamento (UE) 2019/881. Tali atti delegati sono adottati qualora siano stati individuati livelli insufficienti di cibersicurezza e includono un periodo di attuazione. Prima di adottare tali atti delegati, la Commissione effettua una valutazione d'impatto e procede a consultazioni conformemente all'articolo 56 del regolamento (UE) 2019/881. 3. Qualora non siano disponibili sistemi di europei di certificazione della cibersicurezza adeguati ai fini del paragrafo 2 del presente articolo, la Commissione può chiedere all'ENISA, previa consultazione del gruppo di cooperazione e del gruppo europeo per la certificazione della cibersicurezza, di preparare una proposta di sistema a norma dell'articolo 48, paragrafo 2, del regolamento (UE) 2019/881.	
Articolo 25 **Normazione** 1. Per promuovere l'attuazione convergente dell'articolo 21, paragrafi 1 e 2, gli Stati membri, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, incoraggiano l'uso di norme e specifiche tecniche europee e internazionali relative alla sicurezza dei sistemi informatici e di rete. 2. L'ENISA, in cooperazione con gli Stati membri e, se opportuno, previa consultazione dei pertinenti portatori di interessi, elabora documenti di consulenza e orientamento riguardanti tanto i settori tecnici da prendere in considerazione in relazione al paragrafo 1, quanto le norme già esistenti, comprese le norme nazionali, che potrebbero essere applicate a tali settori.	**ART. 28** ***(Specifiche tecniche)*** Confronta anche: **- ART. 31 (*Proporzionalità e gradualità degli obblighi*)** **- ART. 32 *(Previsioni settoriali specifiche)***
CAPO V **GIURISDIZIONE E REGISTRAZIONE**	
Articolo 26 **Giurisdizione e territorialità** 1. I soggetti che rientrano nell'ambito di applicazione della presente direttiva sono considerati sotto la giurisdizione dello Stato membro nel quale sono stabiliti, ad eccezione dei casi seguenti:	**ART. 5** **(Giurisdizione e territorialità)**

a) i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico, che sono considerati sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi; b) i fornitori di servizi 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 considerati sotto la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione a norma del paragrafo 2; c) gli enti della pubblica amministrazione, che sono considerati sotto la giurisdizione dello Stato membro che li ha istituiti. 2. Ai fini della presente direttiva, si considera che un soggetto di cui al paragrafo 1, lettera b), abbia il proprio stabilimento principale nell'Unione nello Stato membro in cui sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio di cibersicurezza. Se non è possibile determinare detto Stato membro o se tali decisioni non sono adottate nell'Unione, lo stabilimento principale è considerato essere nello Stato membro in cui sono effettuate le operazioni di cibersicurezza. Se non è possibile determinare detto Stato membro, si considera che lo stabilimento principale sia nello Stato membro in cui il soggetto interessato ha lo stabilimento con il maggior numero di dipendenti nell'Unione. 3. Se un soggetto di cui al paragrafo 1, lettera b), non è stabilito nell'Unione, ma offre servizi nell'Unione, esso designa un rappresentante nell'Unione. Il rappresentante è stabilito in uno degli Stati membri in cui sono offerti i servizi. Tale soggetto è considerato sotto la giurisdizione dello Stato membro in cui è stabilito il suo rappresentante. Nell'assenza di un rappresentante nell'Unione designato a norma del presente paragrafo, qualsiasi Stato membro in cui il soggetto fornisce servizi può avviare un'azione legale nei confronti del soggetto per	

violazione degli obblighi della presente direttiva. 4. La designazione di un rappresentante da parte di un soggetto di cui al paragrafo 1, lettera b), fa salve le azioni legali che potrebbero essere avviate nei confronti del soggetto stesso. 5. Gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca in relazione a un soggetto di cui al paragrafo 1, lettera b), possono, entro i limiti della richiesta, adottare misure di vigilanza e di esecuzione adeguate in relazione al soggetto interessato che fornisce servizi o che ha un sistema informatico e di rete nel loro territorio.	
Articolo 27 **Registro dei soggetti** 1. L'ENISA crea e mantiene un registro di fornitori di servizi DNS, registri dei nomi di dominio di primo livello, soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, fornitori di servizi di sicurezza gestiti, nonché fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network sulla base delle informazioni ricevute dai punti di contatto unici conformemente al paragrafo 4. Su richiesta, l'ENISA consente alle autorità competenti di accedere a tale registro, assicurando nel contempo la tutela della riservatezza delle informazioni, se del caso. 2. Gli Stati membri esigono che i soggetti di cui al paragrafo 1 trasmettano entro il 17 gennaio 2025, le informazioni seguenti alle autorità competenti: a) il proprio nome; b) il settore, il sottosettore e il tipo di soggetto di cui all'allegato I o II, se del caso; c) l'indirizzo dello stabilimento principale e degli altri stabilimenti legali del soggetto nell'Unione o, se non è stabilito nell'Unione, del suo rappresentante a norma dell'articolo 26, paragrafo 3; d) i dati di contatto aggiornati, compresi gli indirizzi e-mail e i numeri di telefono del soggetto, e, se opportuno, del suo rappresentante a norma dell'articolo 26, paragrafo 3;	**Art. 7, comma 5**

e) gli Stati membri in cui il soggetto fornisce i suoi servizi; e f) le serie di IP del soggetto. 3. Gli Stati membri provvedono affinché i soggetti di cui al paragrafo 1 notifichino all'autorità competente qualsiasi modifica dei dettagli trasmessi a norma del paragrafo 2 tempestivamente e, in ogni caso, entro tre mesi dalla data della modifica. 4. In seguito alla ricezione delle informazioni di cui ai paragrafi 2 e 3, ad eccezione di quelle di cui al paragrafo 2, lettera f), il punto di contatto unico dello Stato membro interessato, senza ritardo, le inoltra all'ENISA. 5. Se opportuno, le informazioni di cui ai paragrafi 2 e 3 del presente articolo sono trasmesse attraverso il meccanismo nazionale di cui all'articolo 3, paragrafo 4, quarto comma.	
Articolo 28 **Banca dati dei dati di registrazione dei nomi di dominio** 1. Per contribuire alla sicurezza, alla stabilità e alla resilienza del DNS, gli Stati membri impongono ai registri dei nomi di TLD e ai soggetti che forniscono servizi di registrazione dei nomi di dominio di raccogliere e mantenere dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati con la dovuta diligenza, conformemente al diritto dell'Unione in materia di protezione dei dati per quanto riguarda i dati personali. 2. Ai fini del paragrafo 1, gli Stati membri esigono che la banca dati dei dati di registrazione dei nomi di dominio contenga 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. Tali informazioni includono: a) il nome di dominio; b) la data di registrazione; c) il nome, l'indirizzo e-mail di contatto e il numero di telefono del soggetto che procede alla registrazione; d) 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.	**ART. 29** ***(Banca dei dati di registrazione dei nomi di dominio)*** Confronta anche: **- ART. 31 (*Proporzionalità e gradualità degli obblighi*)** **- ART. 32 *(Previsioni settoriali specifiche)***

3. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio predispongano politiche e procedure, incluse procedure di verifica, per garantire che le banche dati di cui al paragrafo 1 comprendano informazioni accurate e complete. Gli Stati membri esigono che tali politiche e procedure siano rese pubbliche. 4. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio per i TLD rendano pubblicamente disponibili, senza indebito ritardo dopo la registrazione di un nome di dominio, i dati di registrazione dei nomi di dominio che non sono dati personali. 5. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio, su richiesta legittima e debitamente motivata di legittimi richiedenti l'accesso, forniscano l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione in materia di protezione dei dati. Gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio rispondano senza indebito ritardo e comunque entro 72 ore dalla ricezione delle richieste di accesso. Gli Stati membri esigono che le politiche e le procedure relative alla divulgazione di tali dati siano rese pubbliche. 6. Il rispetto degli obblighi di cui ai paragrafi da 1 a 5 non comportano una duplicazione della raccolta di dati di registrazione dei nomi di dominio. A tal fine, gli Stati membri esigono che i registri dei nomi di TLD e i soggetti che forniscono servizi di registrazione dei nomi di dominio collaborino tra loro.	
CAPO VI **CONDIVISIONE DELLE INFORMAZIONI**	
Articolo 29 **Accordi di condivisione delle informazioni sulla cibersicurezza** 1. Gli Stati membri provvedono affinché i soggetti che rientrano nell'ambito di applicazione della presente direttiva e, se del caso, altri soggetti che non rientrano nell'ambito di applicazione della presente direttiva siano in	**ART. 17** ***(Accordi di condivisione delle informazioni sulla sicurezza informatica)***

grado di scambiarsi, su base volontaria, pertinenti informazioni sulla cibersicurezza, comprese informazioni relative a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di cibersicurezza e raccomandazioni concernenti la configurazione degli strumenti di cibersicurezza per individuare le minacce informatiche, se tale condivisione di informazioni: a) mira a prevenire o rilevare gli incidenti, a riprendersi dagli stessi o ad attenuarne l'impatto; b) aumenta il livello di cibersicurezza, 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 attenuazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati. 2. Gli Stati membri provvedono affinché lo scambio di informazioni avvenga nell'ambito di comunità di soggetti essenziali e importanti e, se opportuno, dei loro fornitori o fornitori di servizi. Tale scambio è attuato mediante accordi di condivisione delle informazioni sulla cibersicurezza che tengono conto della natura potenzialmente sensibile delle informazioni condivise. 3. Gli Stati membri facilitano la conclusione degli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 del presente articolo. Gli Stati membri possono 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. Nello stabilire i dettagli relativi alla partecipazione delle autorità pubbliche a tali accordi, gli Stati membri possono imporre condizioni per le informazioni messe a disposizione dalle autorità competenti o dai CSIRT. Gli Stati membri offrono assistenza per l'applicazione di tali accordi conformemente	

alle loro misure strategiche di cui all'articolo 7, paragrafo 2, lettera h). 4. Gli Stati membri provvedono affinché i soggetti essenziali e importanti notifichino alle autorità competenti la loro partecipazione agli accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 al momento della conclusione di tali accordi o, se opportuno, del loro ritiro da tali accordi, una volta che questo è divenuto effettivo. 5. L'ENISA offre assistenza per la conclusione di accordi di condivisione delle informazioni sulla cibersicurezza di cui al paragrafo 2 fornendo orientamenti e provvedendo allo scambio delle migliori pratiche.	
Articolo 30 **Notifica volontaria di informazioni pertinenti** 1. Gli Stati membri provvedono affinché, in aggiunta all'obbligo di notifica di cui all'articolo 23, possano essere trasmesse, su base volontaria, notifiche ai CSIRT o, se opportuno, alle autorità competenti, da parte dei: a) soggetti essenziali e importanti, per quanto riguarda gli incidenti, le minacce informatiche e i quasi incidenti; b) soggetti diversi da quelli di cui alla lettera a), indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione della presente direttiva, per quanto riguarda gli incidenti significativi, le minacce informatiche e i quasi incidenti. 2. Gli Stati membri trattano le notifiche di cui al paragrafo 1 del presente articolo secondo la procedura di cui all'articolo 23. Gli Stati membri possono trattare le notifiche obbligatorie prioritariamente rispetto alle notifiche volontarie. Se necessario, i CSIRT e, se del caso, le autorità competenti forniscono ai punti di contatto unici le informazioni sulle notifiche ricevute a norma del presente articolo, garantendo nel contempo la riservatezza e la tutela adeguata delle informazioni fornite dal soggetto notificante. Fatti salvi la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, la segnalazione volontaria non ha l'effetto di imporre al soggetto notificante alcun obbligo	**ART. 26** ***(Notifica volontaria di informazioni pertinenti)***

aggiuntivo a cui non sarebbe stato sottoposto se non avesse trasmesso la notifica.	
CAPO VII **VIGILANZA ED ESECUZIONE**	
Articolo 31 **Aspetti generali relativi alla vigilanza e all'esecuzione** 1. Gli Stati membri provvedono affinché le proprie autorità competenti monitorino efficacemente e adottino le misure necessarie a garantire il rispetto della presente direttiva. 2. Gli Stati membri possono consentire alle proprie autorità competenti di conferire priorità ai compiti di vigilanza. Tale priorità si fonda su un approccio basato sul rischio. A tal fine, nell'esercizio dei rispettivi compiti di vigilanza di cui agli articoli 32 e 33, le autorità competenti possono stabilire metodologie di vigilanza che consentano di conferire priorità a tali compiti secondo un approccio basato sul rischio. 3. Le autorità competenti operano in stretta cooperazione con le autorità di controllo ai sensi del regolamento (UE) 2016/679 nei casi di incidenti che comportano violazioni di dati personali, senza pregiudicare la competenza e i compiti delle autorità di controllo di cui a tale regolamento. 4. Fatti salvi i quadri legislativi e istituzionali nazionali, gli Stati membri provvedono affinché nel vigilare sul rispetto, da parte degli enti della pubblica amministrazione, della presente direttiva e nell'imporre misure di esecuzione in caso di violazione della presente direttiva, le autorità competenti dispongano dei poteri adeguati per svolgere tali compiti con indipendenza operativa rispetto agli enti della pubblica amministrazione sottoposti a vigilanza. Gli Stati membri possono decidere di imporre misure di vigilanza e di esecuzione adeguate, proporzionate ed efficaci in relazione a tali enti conformemente ai quadri legislativi e istituzionali nazionali.	**ART. 34** ***(Principi generali per lo svolgimento delle attività di vigilanza ed esecuzione)***
Articolo 32 **Misure di vigilanza e di esecuzione relative a soggetti essenziali** 1. Gli Stati membri provvedono affinché le misure di vigilanza o di esecuzione imposte ai	**ART. 35** ***(Monitoraggio, analisi e supporto)***

soggetti essenziali per quanto riguarda gli obblighi di cui alla presente direttiva siano effettive, proporzionate e dissuasive, tenuto conto delle circostanze di ciascun singolo caso. 2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporre tali soggetti come minimo a: a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati; b) audit sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente; c) audit ad hoc, ivi incluso in casi giustificati da un incidente significativo o da una violazione della presente direttiva da parte del soggetto essenziale; d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato; e) richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cibersicurezza adottate dal soggetto interessato, comprese le politiche di cibersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti a norma dell'articolo 27; f) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei compiti di vigilanza; g) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova. Gli audit sulla sicurezza mirati di cui al primo comma, lettera b), si basano su valutazioni del rischio effettuate dall'autorità competente o dal soggetto sottoposto ad audit o su altre informazioni disponibili in materia di rischi. I risultati di eventuali audit sulla sicurezza mirati sono messi a disposizione dell'autorità competente. I costi di tale audit sulla sicurezza mirato svolto da un organismo indipendente sono a carico del soggetto sottoposto ad audit,	**ART. 36** ***(Verifiche e ispezioni)*** **ART. 37** ***(Misure di esecuzione)***

salvo in casi debitamente giustificati in cui l'autorità competente decida altrimenti. 3. Nell'esercizio dei loro poteri di cui al paragrafo 2, lettera e), f) o g), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste. 4. Gli Stati membri provvedono affinché le proprie autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti essenziali, abbiano il potere come minimo di: a) emanare avvertimenti relativi a violazioni della presente direttiva da parte dei soggetti interessati; b) adottare istruzioni vincolanti, ivi incluso per quanto riguarda le misure richieste per evitare il verificarsi di un incidente o porvi rimedio, nonché i termini per l'attuazione di tali misure e per riferire in merito alla loro attuazione, o un'ingiunzione che impongano ai soggetti interessati di porre rimedio alle carenze individuate o alle violazioni della direttiva; c) imporre ai soggetti interessati di porre termine al comportamento che viola la presente direttiva e di astenersi dal ripeterlo; d) imporre ai soggetti interessati di provvedere affinché le loro misure di gestione del rischio di cibersicurezza siano conformi all'articolo 21 o di adempiere gli obblighi di segnalazione di cui all'articolo 23 in una maniera ed entro un termine specificati; e) imporre ai soggetti interessati di informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività che sono potenzialmente interessati da una minaccia informatica significativa in merito alla natura della minaccia, nonché in merito alle eventuali misure protettive o correttive che possano essere adottate da tali persone fisiche o giuridiche in risposta a tale minaccia; f) imporre ai soggetti interessati di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole; g) designare un funzionario addetto alla sorveglianza con compiti ben definiti nell'arco di un periodo di tempo determinato al fine di vigilare sul rispetto degli articoli 18 e 20;	

h) imporre ai soggetti interessati di rendere pubblici gli aspetti delle violazioni della presente direttiva in una maniera specificata; i) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo il diritto nazionale, di una sanzione amministrativa pecuniaria a norma dell'articolo 34, in aggiunta a qualsiasi delle misure di cui al presente paragrafo, lettere da a) a h). 5. Qualora le misure di esecuzione adottate a norma del paragrafo 4, lettere da a) a d), e lettera f), si rivelino inefficaci, gli Stati membri provvedono affinché le proprie autorità competenti abbiano il potere di fissare un termine entro il quale il soggetto essenziale è tenuto ad adottare le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni di tali autorità. Se le misure richieste non sono adottate entro il termine stabilito, gli Stati membri provvedono affinché le proprie autorità competenti abbiano il potere di: a) sospendere temporaneamente o chiedere a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, secondo il diritto nazionale, di sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale; b) chiedere che gli organismi o gli organi giurisdizionali pertinenti, secondo il diritto nazionale, vietino temporaneamente a qualsiasi persona che svolga funzioni dirigenziali a livello di amministratore delegato o rappresentante legale in tale soggetto essenziale di svolgere funzioni dirigenziali in tale soggetto. Le sospensioni o i divieti temporanei a norma del presente paragrafo sono applicati solo finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle prescrizioni dell'autorità competente per le quali le misure di esecuzione sono state applicate. L'imposizione di tali sospensioni o divieti temporanei è soggetta a garanzie procedurali appropriate in conformità ai principi generali del diritto dell'Unione e della Carta, inclusi il diritto a un ricorso effettivo e ad	

un giusto processo, la presunzione di innocenza e i diritti della difesa. Le misure di esecuzione previste dal presente paragrafo non sono applicabili agli enti della pubblica amministrazione che sono soggetti alla presente direttiva. 6. Gli Stati membri provvedono affinché qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale sulla base del potere di rappresentarlo, dell'autorità di prendere decisioni per suo conto o dell'autorità di esercitare un controllo su di esso abbia il potere di garantirne il rispetto della presente direttiva. Gli Stati membri provvedono affinché tali persone fisiche possano essere ritenute responsabili dell'inadempimento dei loro doveri di garantire il rispetto della presente direttiva. Per quanto riguarda gli enti della pubblica amministrazione, il presente paragrafo lascia impregiudicato il diritto nazionale in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati. 7. Nell'adottare qualsiasi misura di esecuzione di cui al paragrafo 4 o 5, le autorità competenti rispettano i diritti della difesa e tengono conto delle circostanze di ciascun singolo caso e almeno degli elementi seguenti: a) la gravità della violazione e l'importanza delle disposizioni violate, essendo le violazioni seguenti, tra l'altro, da considerarsi gravi: i) le violazioni ripetute; ii) la mancata notifica di incidenti significativi o il mancato rimedio a tali incidenti; iii) il mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dalle autorità competenti; iv) l'ostacolo degli audit o delle attività di monitoraggio imposte dall'autorità competente a seguito del rilevamento di una violazione; v) la fornitura di informazioni false o gravemente inesatte relative alle misure in materia di gestione o segnalazione del rischio di cibersicurezza di cui agli articoli 21 e 23; b) la durata della violazione; c) eventuali precedenti violazioni pertinenti commesse dal soggetto interessato;	

d) qualsiasi danno materiale o immateriale causato, incluse le perdite finanziarie o economiche, gli effetti sugli altri servizi e il numero di utenti interessati; e) un'eventuale condotta intenzionale o negligenza da parte dell'autore della violazione; f) qualsiasi misure adottata dal soggetto per prevenire o attenuare il danno materiale o immateriale; g) qualsiasi adesione a codici di condotta o meccanismi di certificazione approvati; h) il livello di collaborazione delle persone fisiche o giuridiche ritenute responsabili con le autorità competenti. 8. Le autorità competenti espongono nei particolari la motivazione delle loro misure di esecuzione. Prima di adottare tali misure le autorità competenti notificano ai soggetti interessati le loro conclusioni preliminari. Esse concedono inoltre a tali soggetti un tempo ragionevole per presentare osservazioni, salvo in casi debitamente giustificati in cui ciò impedirebbe di agire con immediatezza per prevenire un incidente o rispondervi. 9. Gli Stati membri provvedono affinché le loro autorità competenti di cui alla presente direttiva informino le autorità competenti pertinenti all'interno dello stesso Stato membro a norma della direttiva (UE) 2022/2557 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi stabiliti dalla presente direttiva da parte di un soggetto identificato come critico a norma della direttiva (UE) 2022/2557. Se del caso, le autorità competenti di cui alla direttiva (UE) 2022/2557 possono chiedere alle autorità competenti di cui alla presente direttiva di esercitare i propri poteri di vigilanza e di esecuzione in relazione a un soggetto che è stato individuato come soggetto critico ai sensi della direttiva (UE) 2022/2557. 10. Gli Stati membri provvedono affinché le loro autorità competenti ai sensi della presente direttiva cooperino con le pertinenti autorità competenti dello Stato membro interessato a norma del regolamento (UE) 2022/2554. In particolare, gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino il forum di	

sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dalla presente direttiva da parte di un soggetto essenziale designato come fornitore terzo critico di servizi di TIC a norma dell'articolo 31 del regolamento (UE) 2022/2554.	
Articolo 33 **Vigilanza ed esecuzione relative a soggetti essenziali** 1. Se ricevono elementi di prova, indicazioni o informazioni secondo cui un soggetto importante non rispetta presumibilmente la presente direttiva, in particolare dagli articoli 21 e 23 della medesima, gli Stati membri provvedono affinché le autorità competenti intervengano, se necessario, mediante misure di vigilanza ex post. Gli Stati membri provvedono affinché tali misure siano efficaci, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso. 2. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi compiti di vigilanza nei confronti dei soggetti importanti, abbiano il potere di sottoporre tali soggetti come minimo a: a) ispezioni in loco e vigilanza ex post a distanza, effettuate da professionisti formati; b) audit sulla sicurezza mirati svolti da un organismo indipendente o da un'autorità competente; c) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario, con la cooperazione del soggetto interessato; d) richieste di qualsiasi informazione necessaria a valutare ex post le misure di gestione dei rischi di cibersicurezza adottate dal soggetto, comprese le politiche di cibersicurezza documentate, nonché il rispetto degli obblighi di trasmettere informazioni alle autorità competenti a norma dell'articolo 27; e) richieste di accesso a dati, documenti e/o informazioni necessari allo svolgimento dei propri compiti di vigilanza;	**ART. 35** ***(Monitoraggio, analisi e supporto)***

f) richieste di dati che dimostrino l'attuazione di politiche di cibersicurezza, quali i risultati di audit sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova. Gli audit sulla sicurezza mirati di cui al primo comma, lettera b), si basano su valutazioni del rischio effettuate dall'autorità competente o dal soggetto sottoposto ad audit o su altre informazioni disponibili in materia di rischi. I risultati di eventuali audit sulla sicurezza mirati sono messi a disposizione dell'autorità competente. I costi di tale audit sulla sicurezza mirato svolto da un organismo indipendente sono a carico del soggetto sottoposto a audit, salvo in casi debitamente giustificati in cui l'autorità competente decida altrimenti. 3. Nell'esercizio dei loro poteri a norma del paragrafo 2, lettere d), e) o f), le autorità competenti dichiarano la finalità della richiesta e specificano le informazioni richieste. 4. Gli Stati membri provvedono affinché le autorità competenti, nell'esercizio dei rispettivi poteri di esecuzione nei confronti dei soggetti importanti, abbiano il potere come minimo di: a) emanare avvertimenti relativi a violazioni della presente direttiva da parte dei soggetti interessati; b) adottare istruzioni vincolanti o un'ingiunzione che impongano a tali soggetti di porre rimedio alle carenze individuate o alle violazioni degli obblighi della presente direttiva; c) imporre ai soggetti interessati di porre termine alle condotte in violazione della presente direttiva e di astenersi dal ripeterle; d) imporre ai soggetti interessati di provvedere affinché le loro misure di gestione dei rischi di cibersicurezza siano conformi all'articolo 21 o i loro obblighi di segnalazione conformi alle prescrizioni di cui all'articolo 23 in una maniera ed entro un termine specificati; e) imporre ai soggetti interessati di informare le persone fisiche o giuridiche cui forniscono servizi o per cui svolgono attività potenzialmente interessati da una minaccia informatica significativa in merito alla natura della minaccia e alle eventuali misure protettive o correttive che possano essere adottate da tali	

persone fisiche o giuridiche in risposta a tale minaccia; f) imporre agli interessati di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza entro un termine ragionevole; g) imporre ai soggetti interessati di rendere pubblici gli aspetti delle violazioni della presente direttiva in una maniera specificata; h) imporre o chiedere l'imposizione, da parte degli organismi o degli organi giurisdizionali pertinenti secondo la legislazione nazionale, di una sanzione amministrativa pecuniaria a norma dell'articolo 34, in aggiunta a una qualsiasi delle misure di cui al presente paragrafo, lettere da a) a g). 5. L'articolo 32, paragrafi 6, 7 e 8, si applica *mutatis mutandis* alle misure di vigilanza ed esecuzione di cui al presente articolo per soggetti importanti. 6. Gli Stati membri provvedono affinché le loro autorità competenti ai sensi della presente direttiva cooperino con le pertinenti autorità competenti dello Stato membro interessato a norma del regolamento (UE) 2022/2554. In particolare, gli Stati membri provvedono affinché le loro autorità competenti a norma della presente direttiva informino il forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercitano i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dalla presente direttiva da parte di un soggetto importante designato come fornitore terzo critico di servizi di TIC a norma dell'articolo 31 del regolamento (UE) 2022/2554.	
Articolo 34 **Condizioni generali per imporre sanzioni amministrative pecuniarie ai soggetti essenziali e importanti** 1. Gli Stati membri provvedono affinché le sanzioni amministrative pecuniarie imposte ai soggetti essenziali e importanti a norma del presente articolo in relazione alle violazioni della presente direttiva siano effettive, proporzionate e dissuasive, tenendo conto delle circostanze di ogni singolo caso.	**ART. 38** ***(Sanzioni amministrative)***

2. Le sanzioni amministrative pecuniarie sono imposte in aggiunta a qualsiasi delle misure di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g). 3. Nel decidere se imporre una sanzione amministrativa pecuniaria e il relativo importo in ciascun singolo caso si tiene debitamente conto almeno degli elementi di cui all'articolo 32, paragrafo 7. 4. Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti essenziali siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 10 000 000 EUR o a un massimo di almeno il 2 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore. 5. Gli Stati membri provvedono affinché, ove violino l'articolo 21 o 23, i soggetti importanti siano soggetti, conformemente ai paragrafi 2 e 3 del presente articolo, a sanzioni pecuniarie amministrative pari a un massimo di almeno 7 000 000 EUR o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore. 6. Gli Stati membri possono prevedere la facoltà di infliggere penalità di mora al fine di imporre a un soggetto essenziale o importante di cessare una violazione della presente direttiva conformemente a una precedente decisione dell'autorità competente. 7. Fatti salvi i poteri delle autorità competenti a norma degli articoli 32 e 33, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere imposte sanzioni amministrative pecuniarie agli enti della pubblica amministrazione. 8. Se l'ordinamento giuridico di uno Stato membro non prevede sanzioni amministrative pecuniarie, lo Stato membro in questione provvede affinché il presente articolo possa applicarsi in maniera tale che l'azione sanzionatoria sia avviata dall'autorità competente e la sanzione pecuniaria sia irrogata	

dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità competenti. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Lo Stato membro notifica alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il 17 ottobre 2024 e ne comunicano senza ritardo ogni successiva modifica.	
Articolo 35 **Violazioni che comportano una violazione dei dati personali** 1. Qualora le autorità competenti, in sede di vigilanza o di esecuzione, vengano a conoscenza del fatto che la violazione degli obblighi di cui agli articoli 21 e 23 della presente direttiva da parte di un soggetto essenziale o importante possa comportare una violazione dei dati personali, quale definita all'articolo 4, punto 12), del regolamento (UE) 2016/679, che deve essere notificata a norma dell'articolo 33 del medesimo regolamento, ne informano senza indebito ritardo le autorità di controllo competenti a norma dell'articolo 55 o 56 di tale regolamento. 2. Qualora le autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del medesimo regolamento, le autorità competenti non impongono una sanzione amministrativa pecuniaria a norma dell'articolo 34 della presente direttiva per una violazione di cui al presente articolo, paragrafo 1, imputabile al medesimo comportamento punito con l'ammenda amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del regolamento (UE) 2016/679. Le autorità competenti possono tuttavia imporre le misure di esecuzione di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g) della presente direttiva. 3. Qualora l'autorità di controllo competente a norma del regolamento (UE) 2016/679 sia stabilita in uno Stato membro diverso rispetto	**Articolo 14** **(Cooperazione tra Autorità nazionali)**

all'autorità competente, l'autorità competente informa l'autorità di controllo stabilita nel proprio Stato membro della potenziale violazione dei dati personali di cui al paragrafo 1.	
Articolo 36 **Sanzioni** Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle misure nazionali adottate in attuazione della presente direttiva e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Gli Stati membri comunicano alla Commissione, entro il 17 gennaio 2025, tali norme e misure e la informano, immediatamente, di qualsiasi modifica apportata successivamente.	**ART. 38** ***(Sanzioni amministrative)***
Articolo 37 **Assistenza reciproca** 1. Se un soggetto fornisce servizi in più di uno Stato membro o fornisce servizi in uno o più Stati membri e i suoi sistemi informatici e di rete sono ubicati in uno o più altri Stati membri, le autorità competenti degli Stati membri interessati cooperano e si assistono reciprocamente in funzione delle necessità. Tale cooperazione comprende, almeno, gli aspetti seguenti: a) le autorità competenti che applicano misure di vigilanza o di esecuzione in uno Stato membro informano e consultano, attraverso il punto di contatto unico, le autorità competenti degli altri Stati membri interessati in merito alle misure di vigilanza ed esecuzione adottate; b) un'autorità competente può chiedere a un'altra autorità competente di adottare misure di vigilanza o esecuzione; c) un'autorità competente, dopo aver ricevuto una richiesta giustificata da un'altra autorità competente, fornisce a tale altra autorità competente un'assistenza reciproca proporzionata alle proprie risorse affinché le misure di vigilanza o esecuzione possano essere attuate in maniera efficace, efficiente e coerente. L'assistenza reciproca di cui al primo comma. Lettera c), può riguardare richieste di informazioni e misure di vigilanza, comprese	**ART. 39** ***(Assistenza reciproca)***

richieste di effettuare ispezioni in loco o vigilanza a distanza o audit sulla sicurezza mirati. Un'autorità competente destinataria di una richiesta di assistenza non può respingerla a meno che non abbia stabilito che essa non è competente per fornire l'assistenza richiesta, che l'assistenza richiesta non è proporzionata ai compiti di vigilanza svolti dall'autorità competente o che la richiesta riguarda informazioni o comporta attività che, se divulgate o svolte, sarebbero contrari agli interessi essenziali della sicurezza nazionale, la pubblica sicurezza o la difesa dello Stato membro in questione. Prima di respingere tale richiesta, l'autorità competente consulta le altre autorità competenti interessate e, su richiesta di uno degli Stati membri interessati, la Commissione e l'ENISA, 2. Se opportuno e di comune accordo le autorità competenti di diversi Stati membri possono svolgere le attività di vigilanza comuni.	
CAPO VIII **ATTI DELEGATI E ATTI DI ESECUZIONE**	
Articolo 38 **Esercizio della delega** 1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo. 2. Il potere di adottare atti delegati di cui all'articolo 24, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 16 gennaio 2023. 3. La delega di potere di cui all'articolo 24, paragrafo 2, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella Gazzetta ufficiale dell'Unione europea o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore. 4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016. 5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.	*Non richiede recepimento*

6. L'atto delegato adottato a norma dell'articolo 24, paragrafo 2, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.	
Articolo 39 **Procedura di comitato** 1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011. 2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011. 3. Laddove il parere del comitato debba essere ottenuto con procedura scritta, questa si conclude senza esito quando, entro il termine per la formulazione del parere, il presidente del comitato decida in tal senso o un membro del comitato lo richieda.	*Non richiede recepimento*
CAPO IX **DISPOSIZIONI FINALI**	
Articolo 40 **Riesame** Entro il 17 ottobre 2027 e successivamente ogni 36 mesi, la Commissione riesamina il funzionamento della presente direttiva e presenta una relazione in proposito al Parlamento europeo e al Consiglio. La relazione valuta in particolare la pertinenza delle dimensioni dei soggetti interessati, e i settori, sottosettori e tipologie di soggetti di cui agli allegati I e II per il funzionamento dell'economia e della società in relazione alla cibersicurezza. A tal fine e allo scopo di intensificare ulteriormente la cooperazione strategica e operativa, la Commissione tiene conto delle relazioni del gruppo di cooperazione e della rete di CSIRT sull'esperienza acquisita a livello strategico e operativo. La relazione è corredata, se necessario, di una proposta legislativa.	*Non richiede recepimento*

Articolo 41 **Recepimento** 1. Entro il 17 ottobre 2024, gli Stati membri adottano e pubblicano le misure necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni. Essi applicano tali disposizioni a decorrere dal 18 ottobre 2024. 2. Le disposizioni di cui al paragrafo 1 adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.	
Articolo 42 **Modifica del regolamento (UE) n. 910/2014** Nel regolamento (UE) n. 910/2014, l'articolo 19 è soppresso con effetto a decorrere dal 18 ottobre 2024.	
Articolo 43 **Modifica della direttiva (UE) 2018/1972** Nella direttiva (UE) 2018/1972, gli articoli 40 e 41 sono soppressi. con effetto a decorrere dal 18 ottobre 2024.	
Articolo 44 **Abrogazione** La direttiva (UE) 2016/1148 è abrogata con effetto a decorrere dal 18 ottobre 2024. I riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva e vanno letti secondo la tavola di concordanza di cui all'allegato III.	**ART. 41** ***(Abrogazioni e regime transitorio)***
	ART. 43 ***(Modifiche normative)*** *coordinamento*
Articolo 45 **Entrata in vigore** La presente direttiva entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.	*Non richiede recepimento*
Articolo 46 **Destinatari**	*Non richiede recepimento*

Gli Stati membri sono destinatari della presente direttiva.	
	ART. 11 ***(Autorità di settore NIS)*** *In attuazione dell'articolo 3, comma 1, lettera d), della legge 21 febbraio 2024, n. 15 - legge di delegazione europea 2022-2023* **ART. 12** ***(Tavolo per l'attuazione della disciplina NIS)*** **ART. 33** ***(Coordinamento con la disciplina del Perimetro di sicurezza nazionale cibernetica)*** *In attuazione dell'articolo 3, comma 1, lettera p), della legge 21 febbraio 2024, n. 15 - legge di delegazione europea 2022-2023* ***ART. 40*** ***(Attuazione)***
Allegato I SETTORI AD ALTA CRITICITÀ **1. Energia** Sotto settore a) Energia elettrica Tipo di soggetto — Impresa elettrica quale definita all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio che esercita attività di «fornitura» quale definita all'articolo 2, punto 12), di tale direttiva — Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944 — Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944	**ALLEGATO I** **Settori ad altra criticità**

— Produttori quali definiti all’articolo 2, punto 38), della direttiva (UE) 2019/944 — Gestori del mercato elettrico designato quali definiti all’articolo 2, punto 8), del regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio —Partecipanti al mercato dell’energia elettrica quali definiti all’articolo 2, punto 25), del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia quali definiti all’articolo 2, punti 18), 20) e 59) della direttiva (UE) 2019/944 —Gestori di un punto di ricarica responsabili della gestione e del funzionamento di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità Sotto settore b) Teleriscaldamento e teleraffrescamento Tipo di soggetto — Gestori di teleriscaldamento o teleraffrescamento quali definiti all’articolo 2, punto 19), della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio Sotto settore c) Petrolio Tipo di soggetto — Gestori di oleodotti — Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio — Organismi centrali di stoccaggio quali definiti all’articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio Sotto settore d) Gas Tipo di soggetto — Imprese fornitrici quali definite all’articolo 2, punto 8), della direttiva 2009/73/CE del Parlamento europeo e del Consiglio — Gestori del sistema di distribuzione quali definiti all’articolo 2, punto 6), della direttiva 2009/73/CE	

— Gestori del sistema di trasporto quali definiti all'articolo 2, punto 4), della direttiva 2009/73/CE — Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10), della direttiva 2009/73/CE — Gestori del sistema GNL quali definiti all'articolo 2, punto 12), della direttiva 2009/73/CE — Imprese di gas naturale quali definite all'articolo 2, punto 1), della direttiva 2009/73/CE; — Gestori di impianti di raffinazione e trattamento di gas naturale Sotto settore e) Idrogeno Tipo di soggetto — Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno **2. Trasporti** Sotto settore a) Trasporto aereo Tipo di soggetto — Vettori aerei quali definiti all'articolo 3, punto 4), del regolamento (CE) n. 300/2008 utilizzati a fini commerciali —Gestori aeroportuali quali definiti all'articolo 2, punto 2), della direttiva 2009/12/CE del Parlamento europeo e del Consiglio, aeroporti quali definiti all'articolo 2, punto 1), di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, e soggetti che gestiscono impianti annessi situati in aeroporti —Operatori attivi nel controllo della gestione del traffico che forniscono un servizio di controllo del traffico aereo quali definiti all'articolo 2, punto 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio Sotto settore b) Trasporto ferroviario Tipo di soggetto	

— Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio — Imprese ferroviarie quali definiti all'articolo 3, punto 1), della direttiva 2012/34/UE, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, punto 12), di tale direttiva Sotto settore c) Trasporto per vie d'acqua Tipo di soggetto —Compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite per il trasporto marittimo all'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, escluse le singole navi gestite da tale compagnia — Organi di gestione dei porti quali definiti all'articolo 3, punto 1), della direttiva 2005/65/CE del Parlamento europeo e del Consiglio, compresi i relativi impianti portuali quali definiti all'articolo 2, punto 11), del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti —Gestori di servizi di assistenza al traffico marittimo (VTS) quali definiti all'articolo 3, lettera o), della direttiva 2002/59/CE del Parlamento europeo e del Consiglio Sotto settore d) Trasporto su strada Tipo di soggetto — Autorità stradali quali definite all'articolo 2, punto 12), del regolamento delegato (UE) 2015/962 della Commissione responsabili del controllo della gestione del traffico, esclusi i soggetti pubblici per i quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono soltanto una parte non essenziale della loro attività generale — Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1), della direttiva 2010/40/UE del Parlamento europeo e del Consiglio **3. Settore bancario**	

Tipo di soggetto Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio **4. Infrastrutture dei mercati finanziari** Tipo di soggetto —Gestori delle sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio —Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio **5. Settore sanitario** Tipo di soggetto —Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio —Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio — Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio) — Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2 — Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio **6. Acqua potabile** Tipi di soggetto Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio, ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo	

umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni **7. Acque reflue** Tipi di soggetto Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale **8. Infrastrutture digitali** Tipo di soggetto — Fornitori di punti di interscambio internet — Fornitori di servizi DNS, esclusi gli operatori dei server dei nomi radice — Registri dei nomi di dominio di primo livello (TLD) — Fornitori di servizi di cloud computing — Fornitori di servizi di data center — Fornitori di reti di distribuzione dei contenuti (content delivery network) — Fornitori di servizi fiduciari — Fornitori di reti pubbliche di comunicazione — Fornitori di servizi di comunicazione elettronica accessibili al pubblico **9. Gestione dei servizi TIC (business-to-business)** Tipo di soggetto — Fornitori di servizi gestiti — Fornitori di servizi di sicurezza gestiti **10. Pubblica amministrazione** Tipo di soggetto - Enti della pubblica amministrazione delle amministrazioni centrali quali definiti da uno Stato membro conformemente al diritto nazionale — Enti della pubblica amministrazione a livello regionale quali definiti da uno Stato membro conformemente al diritto nazionale **11. Spazio** Tipo di soggetto	**ALLEGATO III** **Amministrazioni centrali, regionali, locali e di altro tipo** **ALLEGATO IV** **Ulteriori tipologie di soggetti**

- Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica **ALLEGATO II** **ALTRI SETTORI CRITICI** **1. Servizi postali e di corriere** Tipo di soggetto - Fornitori di servizi postali quali definiti all'articolo 2, punto 1 bis), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere **2. Gestione dei rifiuti** Tipo di soggetto Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, escluse quelle per cui la gestione dei rifiuti non è la principale attività economica **3. Fabbricazione, produzione e distribuzione di sostanze chimiche** Tipo di soggetto - Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele **4. Produzione, trasformazione e distribuzione di alimenti** Tipo di soggetto Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione **5. Fabbricazione** Sotto settore a) Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro Tipo di soggetto	**ALLEGATO II** **Altri settori critici**

- Soggetti che fabbricano dispositivi medici quali definiti all'articolo 2, punto 1), del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio e soggetti che fabbricano dispositivi medico- diagnostici in vitro quali definiti all'articolo 2, punto 2), del regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio ad eccezione dei soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5), quinto trattino, della presente direttiva Sotto settore b) Fabbricazione di computer e prodotti di elettronica e ottica Tipo di soggetto - Imprese che svolgono attività economiche di cui alla sezione C, divisione 26, della NACE Rev. 2 Sotto settore c) Fabbricazione di apparecchiature elettriche Tipo di soggetto - Imprese che svolgono attività economiche di cui alla sezione C, divisione 27, della NACE Rev. 2 Sotto settore d) Fabbricazione di macchinari e apparecchiature n.c.a. Tipo di soggetto - Imprese che svolgono attività economiche di cui alla sezione C, divisione 28, della NACE Rev. 2 Sotto settore e) Fabbricazione di autoveicoli, rimorchi e semirimorchi Tipo di soggetto - Imprese che svolgono attività economiche di cui alla sezione C, divisione 29, della NACE Rev. 2 Sotto settore f) Fabbricazione di altri mezzi di trasporto Tipo di soggetto - Imprese che svolgono attività economiche di cui alla sezione C, divisione 30, della NACE Rev. 2 **6. Fornitori di servizi digitali**	

Tipo di soggetto — Fornitori di mercati online — Fornitori di motori di ricerca online — Fornitori di piattaforme di servizi di social network **7. Ricerca** Tipo di soggetto Organizzazioni di ricerca	

RELAZIONE TECNICA

Lo schema di decreto legislativo è volto al recepimento della 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 NIS2)*" – che, conseguentemente, abroga a sua volta il d.lgs. 18 maggio 2018, n. 65, di recepimento della direttiva (UE) 2016/1148 (direttiva NIS) – si suddivide in 6 Capi e 44 articoli, riproponendo la struttura della direttiva NIS2 (nel prosieguo, "direttiva") alla luce dei principi e dei criteri introdotti dall'articolo 3 della legge 21 febbraio 2024, n. 15, recante "*Delega al Governo per il recepimento delle direttive europee e* l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2022-2023".

Il **Capo I** (articoli 1-8), recante disposizioni generali, non ha diretti riflessi di natura finanziaria. In particolare:

L'articolo 1 definisce l'oggetto del presente decreto legislativo, confermando, al comma 2, lettera c), l'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS, Punto di contatto unico NIS e Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente (CSIRT Italia) in ambito nazionale. Tali funzioni sono assolte mediante la dotazione annua assegnata all'ACN dall'articolo 18, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109 nei limiti del predetto stanziamento.

Dalla disposizione non derivano oneri a carico della finanza pubblica.

L'articolo 2 contiene le definizioni più ricorrenti nel testo del presente decreto legislativo.

Dalla disposizione, avente carattere ordinamentale, non derivano nuovi o maggiori oneri a carico della finanza pubblica.

L'articolo 3 definisce l'ambito di applicazione del presente schema di decreto legislativo**.**

Dalla disposizione, avente carattere ordinamentale, non derivano nuovi o maggiori oneri a carico della finanza pubblica.

L'articolo 4 reca norme di principio in materia di protezione degli interessi nazionali e commerciali
.

Dalla disposizione, avente carattere ordinamentale, non derivano nuovi o maggiori oneri a carico della finanza pubblica.

L'articolo 5 detta le regole in materia di giurisdizione e territorialità per l'applicazione del presente decreto legislativo.

Dalla disposizione, avente carattere ordinamentale, non derivano nuovi o maggiori oneri a carico della finanza pubblica.

L'articolo 6 individua i "soggetti essenziali ed importanti" in base ai requisiti dimensionali e alla tipologia di prodotti/servizi forniti.

Dalla disposizione, avente carattere ordinamentale, non derivano nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 7** disciplina le modalità di identificazione dei soggetti di cui all'articolo 6 sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS ai fini dello svolgimento delle funzioni attribuite all'Agenzia per la cybersicurezza nazionale.

La milestone M1C1-20 del Piano Nazionale di Ripresa e Resilienza prevede il dispiegamento completo dei servizi nazionali Cyber, con traguardo a dicembre 2024, che naturalmente coinvolge anche i soggetti NIS. In particolare, si fa riferimento alla parte del traguardo descritto quale "interconnessione con il team italiano di risposta agli incidenti di sicurezza informatica (CSIRT)". Tale interconnessione viene realizzata attraverso lo sviluppo di un'unica piattaforma digitale, rivolta, anche per ragioni di razionalizzazione ed efficientamento delle risorse e dei servizi offerti, a tutta la constituency dell'Agenzia per la cybersicurezza nazionale. Una componente di tale sviluppo sarà espressamente dedicata alle esigenze "NIS", con un costo specifico stimato in circa 110.000 euro, e sarà rilasciata entro settembre 2024, in tempo per il recepimento della Direttiva.

Tramite la medesima piattaforma si garantirà l'interconnessione con il CSIRT Italia da parte degli altri CERT [sia di quelli pubblici che di quelli istituiti presso i soggetti privati], assicurando altresì, con le dovute procedure, l'accesso alle informazioni (dei soggetti NIS2 e da questi caricate tramite la medesima piattaforma) indispensabili per lo svolgimento delle funzioni istituzionali di risposta agli incidenti da parte dei predetti team.

I costi di sviluppo sopra indicati sono a valere sull'investimento 1.5 del PNRR, dedicato allo sviluppo dei servizi Cyber nazionali, ed in particolare del "Working package" (n. 4, "Servizi PSNC e NIS" per attività di potenziamento dei servizi a supporto delle organizzazioni nazionali nell'ambito del PSNC e della NIS, finanziato complessivamente con 14.600.000 euro.

La disposizione non ha effetti sui saldi di finanza pubblica in quanto sono utilizzate le risorse disponibili e a legislazione vigente.

L'articolo 8 detta apposite misure di protezione dei dati personali**.**

Dalla disposizione, avente carattere ordinamentale, non derivano nuovi o maggiori oneri a carico della finanza pubblica.

Il **Capo II** (articoli 9-17) è volto a definire il quadro nazionale di sicurezza informatica.

L'articolo 9 definisce la strategia nazionale di cybersicurezza aggiornando, sulla base delle disposizioni della Direttiva NIS2, quanto già previsto nell'abrogando D. Lgs. 65/2018. ***Agli oneri derivanti dall'attuazione delle misure strategiche, si provvede con le risorse disponibili a legislazione vigente sul Fondo per l'attuazione della Strategia nazionale di cybersicurezza e sul Fondo per la gestione della cybersicurezza, previsti all'articolo 1, comma 899, lettere a) e b) della legge n. 197 del 2022***

L'**articolo 10** definisce la funzione, attribuita all'ACN, di Autorità nazionale competente NIS e di punto di contatto unico NIS.

Al fine di garantire che l'Autorità nazionale competente NIS e il Punto di contatto unico NIS siano dotati di risorse adeguate a svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi del presente decreto, si dispone di personale sufficiente e formato in modo appropriato.

I relativi oneri sono quantificati in 2.000.000 di euro a decorrere dall'anno 2025.

Detti oneri sono così distinti:

- **euro 1.750.000** annui per l'incremento delle risorse finanziarie destinate al personale di cui all'articolo 18, comma 1, del decreto-legge n. 82 del 2021, utili ai fini della rideterminazione della dotazione organica dello stesso da effettuare con le modalità previste dall'articolo 12, comma 5, del richiamato decreto-legge, che prevede la predetta rideterminazione con apposito DPCM di concerto con il Ministro dell'economia e delle finanze.
- **euro 250.000** annui per le attività di formazione specialistica del personale ACN. Al riguardo si evidenzia che ACN già provvede ad attività specialistiche di formazione e che le attività aggiuntive, nei limiti del predetto stanziamento, saranno effettuate da ACN avvalendosi degli strumenti già in essere per le medesime finalità.

A tali oneri si provvede ai sensi dell'articolo 44.

L'**articolo 11** individua le autorità di settore NIS disciplinandone le funzioni ed i settori di competenza.
Occorre ricordare che già con il decreto legislativo 18 maggio 2018, n. 65, di recepimento della direttiva NIS1, erano state identificate quali autorità di settore:

a) il Ministero dello sviluppo economico, per il settore infrastrutture digitali (sottosettori IXP, DNS, TLD, 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 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, come definita dall'articolo 3, comma 1, lettera a), del decreto legislativo 4 marzo 2014, n. 38, 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.

Rispetto al decreto n. 65 del 2018, il presente schema di decreto amplia i compiti ed i settori in cui le predette autorità sono chiamate ad intervenire:

a) il Ministero delle imprese e del made in Italy, oltre al settore delle infrastrutture digitali (numero 8 dell'allegato I), anche i seguenti:

1. il settore dei servizi postali e di corriere (numero 1 dell'allegato II);
2. il settore della fabbricazione, produzione e distribuzione di sostanze chimiche (numero 3 dell'allegato II) sentito il Ministero dell'ambiente e della sicurezza energetica e il Ministero della salute;
3. 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 (numero 5 dell'allegato II);
4. 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 (numero 5 dell'allegato II) sentito il Ministero delle infrastrutture e dei trasporti;
5. i fornitori di servizi digitali (numero 6 dell'allegato II);

b) il Ministero delle infrastrutture e dei trasporti, oltre al settore trasporti (numero 2 dell'allegato I), anche per i soggetti che forniscono servizi di trasporto pubblico locale (numero 1 dell'allegato IV);

c) il Ministero della salute per:

1. il settore sanitario (numero 5 dell'allegato I);
2. il sottosettore fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro, di cui alla lettera a) del settore fabbricazione (numero 5 dell'allegato II);

d) il Ministero dell'ambiente e della sicurezza energetica, oltre al settore energia (numero 1 dell'allegato I) anche per i seguenti settori:

1. fornitura e distribuzione di acqua potabile (numero 6 dell'allegato I);
2. acque reflue (numero 7 dell'allegato I);
3. gestione rifiuti (numero 2 dell'allegato II).

Rispetto a tale elenco, lo schema di decreto in esame identifica ulteriori amministrazioni con funzioni di autorità di settore NIS e, in particolare:

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

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

c) il Ministero dell'università e della ricerca, per il settore ricerca (numero 7 dell'allegato II) e per gli istituti di istruzione che svolgono attività di ricerca (numero 2 dell'allegato IV);

d) il Ministero della cultura, per i soggetti che svolgono attività di interesse culturale (numero 3 dell'allegato IV).

Al fine di garantire l'efficiente ed efficace svolgimento dei compiti assegnati dal presente decreto alle Autorità di settore NIS, l'articolo 44, comma 2, prevede oneri, derivanti dall'articolo 11, pari a euro **409.424** per l'anno 2024 e ad euro **925.695** annui a decorrere dall'anno 2025, A tali oneri si provvede ai sensi dell'articolo 44. Tali risorse potranno essere utilizzate da ciascuna Autorità di settore NIS, ad

eccezione del MEF che ha mantenuto inalterati i propri settori di intervento e le relative funzioni rispetto al decreto n. 65 del 2018 (NIS1), al fine di reclutare, con contratto di lavoro subordinato a tempo indeterminato, n. 2 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, nonché ad avvalersi di personale non dirigenziale 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, ad esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche. All'atto del collocamento fuori ruolo è reso indisponibile, nella dotazione organica dell'amministrazione di provenienza, per tutta la durata del collocamento fuori ruolo, un numero di posti equivalente dal punto di vista finanziario.

Si rappresenta, altresì, che le Autorità di settore NIS, per i rispettivi settori di competenza procedono all'istituzione e al coordinamento dei tavoli settoriali, al fine di contribuire all'efficace e coerente attuazione del presente decreto nonché al relativo monitoraggio. Ai soggetti partecipanti ai tavoli non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati a carico della finanza pubblica.

La quantificazione degli oneri assunzionali è stata effettuata sulla base delle seguenti retribuzioni pro capite:

PCM	Stipendio 12 mensilità CCNL 2016-2018	13^ mens.	Indennità di Presidenza 12 mens.	Totale	Oneri riflessi	Totale retribuzione fondamentale lordo Stato unitario annuo	Retribuzioni accessorie FUP (Flessibilità - art. 15 CCNI) a.l. +Ind. Spec. Org. (art. 18 CCNI) a.l. comprensivo degli oneri	Retribuzione procapite totale lordo stato (A)	incremento contrattuale CCNL 2019-2021 (B)= (A*3,78%)	incremento contrattuale CCNL 2022-2024 C=(A+B)*5,78 %	RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 3,78% CCNL 2019-2021 e 5,78% CCNL 2022-2024	UNITA' AUTORIZZATE	Onere 2024 (rateo 3 mesi)	Onere complessivo (a regime dal 2025)
A1	29.538,98	2.462	7.682,04	39.683	15.230	54.913	25.515	80.428	3.040,18	4.824,47	88.293	2	44.146,41	176.585,64

MINISTERO DELLE IMPRESE E MADE IN ITALY	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)	Incremento contrattuale CCNL 2022-2024 (5,78%)	RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024	UNITA' AUTORIZZATE	Onere 2024 (rateo)	Onere complessivo (a regime dal 2025)
Funzionari	23.501,93	1.958,49	4.528,68	4.213,13	12.887,51	47.089,74	2.721,79	49.811,53	2	24.905,76	99.623,05

MINISTERO DELL'AGRICOLTURA, SOVRANITA' ALIMENTARE E FORESTE	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)	Incremento contrattuale CCNL 2022-2024 (5,78%)	RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024	UNITA' AUTORIZZATE	Onere 2024 (rateo)	Onere complessivo (a regime dal 2025)
Funzionari	23.501,93	1.958,49	4.529,48	2.825,53	12.434,07	45.249,50	2.615,42	47.864,92	2	23.932,46	95.729,84

MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)	Incremento contrattuale CCNL 2022-2024 (5,78%)	RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024	UNITA' AUTORIZZATE	Onere 2024 (rateo)	Onere complessivo (a regime dal 2025)
Funzionari	23.501,93	1.958,49	4.528,68	4.637,54	13.026,29	47.652,93	2.754,34	50.407,27	2	25.203,64	100.814,54

MINISTERO DELLE INFRASTRUTTURE E DEI TRASPORTI	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)	Incremento contrattuale CCNL 2022-2024 (5,78%)	RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024	UNITA' AUTORIZZATE	Onere 2024 (rateo)	Onere complessivo (a regime dal 2025)
Funzionari	23.501,93	1.958,49	4.683,88	1.080,56	11.922,73	43.147,59	2.493,93	45.641,52	2	22.820,76	91.283,04

MINISTERO DELL'UNIVERSITA' E DELLA RICERCA	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)	Incremento contrattuale CCNL 2022-2024 (5,78%)	RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024	UNITA' AUTORIZZATE	Onere 2024 (rateo)	Onere complessivo (a regime dal 2025)
Funzionari	23.501,93	1.958,49	4.529,48	1.878,27	12.124,32	43.992,49	2.542,77	46.535,25	2	23.267,63	93.070,51

MINISTERO DELLA CULTURA	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)	Incremento contrattuale CCNL 2022-2024 (5,78%)	RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024	UNITA' AUTORIZZATE	Onere 2024 (rateo)	Onere complessivo (a regime dal 2025)
Funzionari	23.501,93	1.958,49	4.529,32	5.553,68	13.326,12	48.869,54	2.824,66	51.694,19	2	25.847,10	103.388,39

MINISTERO DELLA SALUTE	Stipendio CCNL 2019-2021	Tredicesima	Indennità di amministrazione	Trattamento economico accessorio (lordo dipendente)	Oneri riflessi 38,38% (32,70% su retribuzione accessoria)	Retribuzione pro capite totale (fondamentale e accessorio - lordo Stato)	Incremento contrattuale CCNL 2022-2024 (5,78%)	RETRIBUZIONE TOTALE PRO CAPITE LORDO STATO - CON INCR. CONTR. 5,78% CCNL 2022-2024	UNITA' AUTORIZZATE	Onere 2024 (rateo)	Onere complessivo (a regime dal 2025)
Funzionari	23.501,93	1.958,49	4.529,48	1.412,38	11.971,97	43.374,25	2.507,03	45.881,28	2	22.940,64	91.762,56

Riepilogo oneri assunzionali

art. 11, c. 2	Oneri assunzionali		Spese funzionamento		Spese Concorsuali	Buoni pasto		Straordinari		TOTALE	
	2024 (rateo)	2025	2024	2025	2024	2024	2025	2024	2025	2024	2025
a) PCM n. 2 unità	44.146,41	176.585,64	10.000,00	1.000,00		770,00	3.080,00	1.482,53	5.930,10		
c) MIMIT n. 2 unità	24.905,76	99.623,05	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
d) MASAF n. 2 unità	23.932,46	95.729,84	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
e) MASE n. 2 unità	25.203,64	100.814,54	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
f) MIT n. 2 unità	22.820,76	91.283,04	10.000,00	1.000,00	100.000,00	770,00	3.080,00	1.245,26	4.981,02		
g) MUR n. 2 unità	23.267,63	93.070,51	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
h) MIC n. 2 unità	25.847,10	103.388,39	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
i) M. Salute n. 2 unità	22.940,64	91.762,56	10.000,00	1.000,00		770,00	3.080,00	1.245,26	4.981,02		
tot	*213.064,39*	*852.257,57*	*80.000,00*	*8.000,00*	*100.000,00*	*6.160,00*	*24.640,00*	*10.199,31*	*40.797,24*	*409.423,70*	*925.694,81*

Di seguito, i criteri di quantificazione dei seguenti costi correlati all'assunzione dei suddetti contingenti di personale:

BUONI PASTO	Buoni pasto mese n. 20 * 7 euro	Costo annuo calcolato su 11 mesi	Unità	Totale anno 2025	Anno 2024 (rateo)
	140	1540	2	3080	513,33

Straordinario PCM	Aliquota oraria lorda standard	Ore di straordinario annue: 120 (10 ore mensili)	Costo straordinari annuo lordo dipendente compeso	totale
2 unità cat. A1	18,62	120	2965,05	5930,10

CALCOLO STRAORDINARIO MINISTERI	
15,64	orario
5,11	oneri riflessi
20,75	totale orario
2.490,51	per 120 ore
34.867,19	14 unità

Si rappresenta, altresì, che le Autorità di settore NIS, per i rispettivi settori di competenza procedono all'istituzione e al coordinamento dei tavoli settoriali, al fine di contribuire all'efficace e coerente attuazione del presente decreto nonché al relativo monitoraggio. Ai soggetti partecipanti ai tavoli non spettano gettoni di presenza, compensi, rimborsi di spese o altri emolumenti comunque denominati

L'articolo 12 reca l'istituzione, in via permanente, del Tavolo per l'attuazione della disciplina NIS2, al fine di assicurare l'implementazione e attuazione del presente decreto legislativo.

L'amministrazione interessata dall'attuazione della disposizione, vi provvederà con le risorse strumentali, finanziarie e umane disponibili a legislazione vigente.

Il comma 6, stabilisce che la partecipazione al Tavolo in parola non dia luogo alla corresponsione di gettoni di presenza, compensi o rimborsi di spese o altri emolumenti, comunque denominati.

Dalla disposizione non derivano nuovi o maggiori oneri a carico della finanza pubblica.

L'**articolo 13** delinea la composizione ed il funzionamento del quadro nazionale di gestione delle crisi informatiche individuando, quali autorità competenti alla gestione degli incidenti e delle crisi

informatiche su vasta scala (Autorità di gestione delle crisi informatiche), di cui all'articolo 9 della direttiva, l'ACN, anche con funzioni di coordinatore ai sensi del paragrafo 2, del medesimo articolo 9, insieme al Ministero della Difesa, ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera g), del presente decreto.

Al fine di garantire che le Autorità nazionali di gestione delle crisi informatiche siano dotate di risorse adeguate a svolgere in modo efficiente ed efficace i compiti assegnati e conseguire in questo modo gli obiettivi del presente decreto, disponendo di personale sufficiente e formato in modo appropriato, è autorizzata una spesa pari a 1.000.000 di euro annui a decorrere dall'anno 2025. A tali oneri si provvede ai sensi dell'articolo 44.

Detti oneri sono così distinti:

- **euro 500.000** da assegnare all'ACN per far fronte ai seguenti oneri di funzionamento:
    - **euro 200.000**, derivanti dalle specifiche funzioni, anche attraverso l'implementazione di strutture tecnologiche utili al coordinamento delle attività di gestione delle crisi cibernetiche su vasta scala e allo scambio informativo in condizioni di sicurezza;
    - **euro 300.000**, derivanti dalle attività necessarie e funzionali alla partecipazione alle esercitazioni a livello europeo e alle attività formative, esercitative e di preparazione a livello nazionale.
- **euro 500.000** da assegnare al Ministero della difesa per i nuovi e maggiori oneri, ripartiti nel seguente modo:
    - **250.000 euro,** nell'ambito del supporto alle attività di sicurezza della *supply chain* strategica della difesa, essenziale per il funzionamento delle capacità operative dello strumento militare, nonché per lo sviluppo ed il potenziamento info-strutturale di canali sicuri di scambio di informazioni.
    - **150.000 euro,** nell'ambito delle attività di difesa dello Stato**.** In particolare, tali risorse risultano necessarie per il potenziamento info-strutturale e capacitivo nei settori della *Cyber Situational Awareness*, monitoraggio; protezione e risposta;
    - **100.000 euro** necessari per la formazione del personale.

L'**articolo 14** definisce le modalità di cooperazione a livello nazionale integrando le previsioni dell'abrogando D.lgs. n. 65 del 2018 con quanto previsto dalla direttiva. La disposizione non determina nuovi o maggiori oneri a carico della finanza pubblica esplicandosi in attività già svolte nell'ambito delle funzioni istituzionali dell'ACN.

L'**articolo 15** disciplina il Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT Italia) già incardinato all'interno di ACN. L'ottimale funzionamento di detta struttura, che ha natura e compiti prettamente operativi, richiede la presenza continua di personale altamente qualificato, nonché di strumenti hardware e software estremamente performanti.

A tal fine, è autorizzata una spesa pari a 2.000.000 di euro annui a decorrere dall'anno 2025. A tali oneri si provvede ai sensi dell'articolo 44.

Gli oneri sono così ripartiti:

- **euro 1.750.000** annui per l'incremento delle risorse finanziarie destinate al personale di cui all'articolo 18, comma 1, del decreto-legge n. 82 del 2021, utili ai fini della rideterminazione della dotazione organica dello stesso da effettuare con le modalità previste dall'articolo 12, comma 5, del richiamato decreto-legge, che prevede la predetta rideterminazione con apposito DPCM di concerto con il Ministro dell'economia e delle finanze.
- **euro 250.000** annui per l'acquisizione di strumenti hardware e software.

.**L'articolo 16** reca disposizioni sulla divulgazione coordinata delle vulnerabilità e attribuisce allo CSIRT Italia il ruolo di coordinatore dei soggetti interessati e di intermediario tra la persona fisica o giuridica che segnala la vulnerabilità e il fabbricante o fornitore di servizi. ***La disposizione non comporta nuovi o maggiori oneri a carico della finanza pubblica poiché dette attività rientrano nell'ambito complessivo dei compiti svolti da CSIRT Italia***,

L'**articolo 17** disciplina gli accordi di condivisione delle informazioni sulla sicurezza informatica tra i soggetti che rientrano nell'ambito di applicazione del presente decreto, che si sostanziano nello scambio di informazioni sulla sicurezza informatica. ***La disposizione, avente e carattere ordinamentale, non reca nuovi o maggiori oneri per la finanza pubblica.***

Il **Capo III** (articoli da 18 a 22) reca disposizioni per la cooperazione a livello dell'Unione e internazionale.

L'**articolo 18** disciplina l'attività del Gruppo di cooperazione NIS, già operante ai sensi dell'abrogando D.lgs. n. 65 del 2018. La disposizione non comporta nuovi o maggiori oneri a carico della finanza pubblica poiché dette attività rientrano nell'ambito complessivo dei compiti istituzionali svolti da ACN.

.

Gli **articoli 19 e 20** regolano rispettivamente la partecipazione dell'Autorità nazionale di gestione delle crisi cibernetiche alla Rete delle organizzazioni di collegamento per le crisi cibernetiche (EU-CyCLONe) e la partecipazione del CSIRT Italia alla rete di CSIRT nazionali.

La disposizione non comporta nuovi o maggiori a carico della finanza pubblica poiché dette attività rientrano nell'ambito complessivo dei compiti svolti dall'Autorità nazionale di gestione delle crisi cibernetiche e dal CSIRT.

L'articolo 21, introduce la procedura di revisione tra pari, ai sensi dell'articolo 19 della Direttiva NIS2.

La disposizione non comporta oneri a carico della finanza pubblica, le attività previste verranno svolte dall'ACN e con le autorità di settore con le risorse umane, strumentali, finanziarie disponibili a legislazione vigente.

L'**articolo 22** individua gli obblighi di comunicazione verso entità 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, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva.

La disposizione non comporta nuovi o maggiori a carico della finanza pubblica poiché dette attività rientrano nell'ambito delle attività istituzionali svolte dalla Presidenza del Consiglio e dall'Agenzia per la cybersicurezza nazionale.

Il **Capo IV** (articoli da 23 a 33) è dedicato agli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente.

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

La disposizione non comporta nuovi o maggiori a carico della finanza pubblica poiché dette attività rientrano nell'ambito delle attività istituzionali svolte dai soggetti pubblici interessati dall'attuazione della disposizione.

I successivi **articoli 24, 25 e 26** individuano, nel dettaglio, rispettivamente gli obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e quelli in materia di notifica, anche volontaria, di incidente.

La disposizione non comporta nuovi o maggiori a carico della finanza pubblica poiché dette attività rientrano nell'ambito delle attività istituzionali svolte dai soggetti pubblici interessati dall'attuazione della disposizione.

L'**articolo 27** consente all'Autorità nazionale competente NIS di imporre, ai sensi della direttiva, ai soggetti essenziali e importanti l'utilizzo di determinati prodotti TIC, servizi TIC e processi TIC.
Dalla disposizione, avente carattere ordinamentale, non derivano oneri a carico della finanza pubblica.

L'**articolo 28** attribuisce alla medesima Autorità la facoltà di promuove l'uso di specifiche tecniche per favorire l'attuazione efficace e armonizzata delle misure di gestione dei rischi di sicurezza cibernetica;

l'**articolo 29** disciplina poi la banca dei dati di registrazione dei nomi di dominio.
Dalle disposizioni, avente carattere ordinamentale, non derivano oneri a carico della finanza pubblica.

L'**articolo 30** regola modalità circa l'iscrizione nell'elenco dei soggetti importanti ed essenziali, tramite la piattaforma digitale prevista dall'articolo 7.
Dalla disposizione, avente carattere ordinamentale, non derivano oneri a carico della finanza pubblica.

L'**articolo 31** stabilisce che l'Autorità nazionale competente NIS preveda criteri di proporzionalità e gradualità obblighi in materia di gestione del rischio di sicurezza cibernetica e di notifica di incidente; l'**articolo 32** detta regole specifiche per le pubbliche amministrazioni centrali, regionali e

locali e per i soggetti essenziali e importanti che forniscono servizi, anche digitali, alle medesime; l'**articolo 33** reca disposizioni di coordinamento della normativa NIS2 con la disciplina del Perimetro di sicurezza nazionale cibernetica. ***Le predette disposizioni, riguardando attività a prevalente carattere di indirizzo e coordinamento, sono svolte sono svolte nell'ambito delle funzioni istituzionali di ACN con risorse umane, strumentali e finanziarie disponibili a legislazione vigente e non determinano nuovi oneri per la finanza pubblica***.

Il **Capo V** (articoli dal 34 al 39) disciplina le attività di monitoraggio, vigilanza ed esecuzione a carico dell'Autorità nazionale competente NIS, con riferimento ai compiti di monitoraggio, di verifica ed ispezioni, all'adozione di misure di esecuzione e all'eventuale irrogazione delle sanzioni.

L'**articolo 34** reca principi generali per lo svolgimento delle attività di supervisione**.**

Dalla disposizione, avente carattere ordinamentale, non derivano oneri a carico della finanza pubblica.

L'**articolo 35** reca le modalità di effettuazione della attività di monitoraggio, analisi e supporto. Tali attività sono svolte da ACN con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.La disposizione, pertanto, ***non determina nuovi o maggiori oneri per la finanza pubblica***.

Gli **articoli 36 e 37**, disciplinano le attività di verifica e ispezione la relativa esecuzione dell'esercizio dei poteri da parte dell'Autorità NIS. ***Tali compiti - già attualmente svolti da ACN nell'ambito della propria attività istituzionale - non determinano nuovi o maggiori oneri.***

L'**articolo 38** reca disposizioni in materia di sanzioni amministrative**.** In particolare, il **comma 16**, prevede che i proventi delle sanzioni amministrative pecuniarie irrogate dall'Autorità nazionale competente NIS versati all'entrata dello Stato siano oggetto di riassegnazione all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze (cap. 1672) recante la dotazione finanziaria da assegnare annualmente all'ACN. La disposizione, peraltro, è pienamente coerente con l'articolo 11, comma 2 del decreto-legge n. 82 del 2021 che, alla lettera f), indica i predetti proventi delle sanzioni tra le entrate dell'Agenzia.

Sul punto si deve specificare, altresì, che l'acquisizione in bilancio di risorse aggiuntive derivanti dalle predette sanzioni rappresenta per l'ACN una mera eventualità; le stesse, infatti, hanno il fine esclusivo di rappresentare un efficace strumento di deterrenza volto a garantire l'attuazione delle misure previste dal provvedimento.

Al riguardo si assicura, infine, che i proventi in discorso rappresentano una nuova voce di entrata del bilancio dello Stato, non essendovi fino ad oggi somme versate per la medesima causale. Pertanto, la previsione di riassegnazione all'ACN degli eventuali introiti ha carattere di neutralità finanziaria e non determina riflessi negativi sui saldi di bilancio.

Il **Capo VI** (articoli da 40 a 44) reca disposizioni finali e transitorie.

L'articolo 40 reca la disciplina di attuazione del provvedimento.

Dalla disposizione non derivano oneri a carico della finanza pubblica

L'**articolo 41** reca disposizioni abrogative. Fa salva la vigenza delle autorizzazioni di spesa di cui agli articoli 7, comma 8, e 8, comma 10, d.lgs. 65/2018 fino al 1 gennaio 2025

In particolare, le risorse rivenienti dall'abrogazione di cui al comma 1 dell'articolo 41, pari 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, sono utilizzate per la copertura di parte degli oneri complessivi indicati all'articolo 44.

L'articolo 42 reca la disciplina di prima applicazione del provvedimento.

Dalla disposizione non derivano oneri a carico della finanza pubblica.

L'articolo 43 reca le modifiche normative necessarie per assicurare la coerenza con l'architettura nazionale di cybersicurezza e con i compiti dell'Agenzia per la cybersicurezza nazionale.

Dalla disposizione non derivano oneri a carico della finanza pubblica.

L'**articolo 44**, reca la disposizione finanziaria degli oneri derivanti dagli articoli 10, 11, 13, comma 1, e 15, pari a 409.424 euro per l'anno 2024 e 5.925.695 euro annui a decorrere dall'anno 2025, a cui 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 di cui all'articolo 41-bis della legge 24 dicembre 2012, n. 234;

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 cui al comma 1 dell'articolo 41.

La verifica della presente relazione tecnica, effettuata ai sensi dell'art. 17 comma 3, della Legge 31 dicembre 2009, n. 196 ha avuto esito **positivo** ☒ negativo ☐

17/06/2024 Il Ragioniere Generale dello Stato
Firmato digitalmente *Biagio Mazzotta*

ANALISI TECNICO-NORMATIVA (A.T.N.)

(Allegato "A" alla direttiva del P.C.M. del 10 settembre 2008 - G.U. n. 219 del 2008)

Amministrazione proponente: Agenzia per la cybersicurezza nazionale. Servizio di Gabinetto, Divisione Affari giuridici, legislativi e legali.

Titolo: *Schema di decreto legislativo di recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.*

PARTE I. ASPETTI TECNICO-NORMATIVI DI DIRITTO INTERNO

1) Obiettivi e necessità dell'intervento normativo. Coerenza con il programma di governo.

Occorre dare attuazione nell'ordinamento nazionale alle disposizioni della direttiva (UE) n.2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, la quale, superando e abrogando la precedente direttiva NIS, reca misure volte a garantire un livello comune elevato di cybersicurezza nell'Unione, al fine di rispondere alle crescenti minacce poste dalla digitalizzazione, rafforzando la sicurezza dei soggetti coinvolti nel processo. In tal senso, la direttiva NIS 2 prevede un ampliamento dell'ambito di applicazione, che obbliga più entità e settori ad adottare misure di sicurezza, includendo, per quanto riguarda il settore pubblico, anche le pubbliche amministrazioni.

Al riguardo, la legge 21 febbraio 2024, n. 15 (Legge di delegazione europea 2022-2023), ha conferito apposita delega legislativa al Governo, da esercitarsi nell'osservanza, oltreché dei principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n.234, anche dei principi e criteri direttivi specifici indicati dall'articolo 3 della medesima legge di delegazione. Tale ultima disposizione:
a) prevede che siano individuati 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, anche considerando la possibilità di applicazione della direttiva medesima ai comuni e alle province secondo principi di gradualità, proporzionalità e adeguatezza;

b) dispone l'esclusione dall'ambito di applicazione delle disposizioni della direttiva (UE) 2022/2555 degli enti della pubblica amministrazione 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 (articolo 2, paragrafo 7, della direttiva medesima), compresi gli organismi di informazione per la sicurezza ai quali si applicano le disposizioni della legge 3 agosto 2007, n. 124;

c) stabilisce la possibilità (cui all'articolo 2, paragrafo 8, della direttiva (UE) 2022/2555) di prevedere che con uno o più DPCM, adottati su proposta delle competenti amministrazioni, siano esentati soggetti specifici che svolgono attività nei settori ivi indicati o che forniscono servizi esclusivamente agli enti della pubblica amministrazione di cui all'articolo 2, paragrafo 7, citati;

d) dispone la conferma della distinzione tra l'Agenzia per la cybersicurezza nazionale, quale autorità nazionale competente e punto di contatto, ai sensi dell'articolo 8 della direttiva (UE) 2022/2555, e le autorità di settore operanti negli ambiti di cui agli allegati I e II alla medesima direttiva;

e) in relazione all'istituzione del team di risposta agli incidenti di sicurezza informatica (CSIRT), di cui all'articolo 10 della direttiva (UE) 2022/2555, stabilisce che siano confermate le disposizioni dell'articolo 8 del decreto legislativo 18 maggio 2018, n. 65, recante attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, in materia di istituzione del CSIRT Italia, nonché che sia ampliato 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;

f) stabilisce che sia previsto un regime transitorio per i soggetti già sottoposti alla disciplina del decreto legislativo 18 maggio 2018, n. 65, garantendo termini congrui di adeguamento, ai fini della migliore applicazione delle disposizioni previste dalla direttiva (UE) 2022/2555;

g) richiede la previsione di meccanismi che consentano la registrazione dei soggetti essenziali e importanti (di cui all'articolo 3 della direttiva (UE) 2022/2555), per la comunicazione dei dati previsti dal paragrafo 4 del medesimo articolo 3, compresi i soggetti che gestiscono servizi connessi o strumentali alle attività oggetto delle disposizioni della direttiva medesima relative al settore della cultura;

h) in relazione alle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555 (ovvero le misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che i soggetti essenziali e importanti adottano ed utilizzano nelle loro attività 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), l'articolo in esameprevede 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. Prevede, altresì, che l'autorità amministrativa individuata come responsabile di tale procedimento provveda anche all'aggiornamento degli strumenti adottati;

i) stabilisce l'introduzione nella legislazione vigente, anche in materia penale, delle modifiche necessarie al fine di assicurare il corretto recepimento nell'ordinamento nazionale delle disposizioni della direttiva (UE) 2022/2555 in materia di divulgazione coordinata delle vulnerabilità;

l) richiede la definizione delle 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 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno;

m) richiede l'individuazione di criteri oggettivi e proporzionati ai fini dell'applicazione degli obblighi informativi di cui all'articolo 23, paragrafo 2, della direttiva (UE) 2022/2555;

n) stabilisce che sia rivisto il sistema sanzionatorio e il sistema di vigilanza ed esecuzione, in particolare:
1) prevedendo sanzioni effettive, proporzionate e dissuasive rispetto alla gravità della violazione degli obblighi derivanti dalla direttiva (UE) 2022/2555, anche in deroga ai criteri e ai limiti previsti

dall'articolo 32, comma 1, lettera d), della legge 24 dicembre 2012, n. 234, e alla legge 24 novembre 1981, n. 689, introducendo strumenti deflativi del contenzioso, quali la diffida ad adempiere;
2) prevedendo che gli introiti derivanti dall'irrogazione delle sanzioni siano 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, di cui all'articolo 18 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale;

o) richiede che sia assicurato il miglior coordinamento tra le disposizioni adottate ai sensi dell' articolo 3 della legge di delegazione europea 2022-2023 per il recepimento della direttiva (UE) 2022/2555, le disposizioni adottate ai sensi dell'articolo 5 della medesima legge per il recepimento della direttiva (UE) 2022/2557 (relativa alla resilienza dei soggetti critici), nonché le disposizioni del regolamento (UE) 2022/2554 (relativo alla resilienza operativa digitale per il settore finanziario) e quelle adottate ai sensi del successivo articolo 16 per l'adeguamento a quest'ultimo e per il recepimento della direttiva (UE) 2022/2556 (che interviene a modificare diverse direttive sempre nell' ambito della resilienza operativa digitale per il settore finanziario);

p) dispone che siano apportate alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il coordinamento con le disposizioni emanate in attuazione dell' articolo 3 della legge 15/2024, in esame.

2) ***Analisi del quadro normativo nazionale.***

Il quadro normativo ordinamentale nazionale relativo agli interventi posti in essere con le disposizioni contenute nel decreto legislativo è così composto:

- decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

Il decreto-legge n. 82 del 2021 ha ridefinito l' architettura nazionale in materia di cybersicurezza ed ha istituito l' Agenzia per la cybersicurezza nazionale.

- decreto legislativo 1° agosto 2003, n. 259.

Il decreto legislativo n. 259 del 2003, recante il codice delle comunicazioni elettroniche, raccoglie la normativa nazionale per il settore dei servizi e del mercato delle telecomunicazioni e delle radiocomunicazioni.

- legge 24 novembre 1981, n. 689.

La legge n. 689 del 1981 reca modifiche al codice penale.

- legge 31 dicembre 2009, n.196

La legge n.196 del 2009 è la legge di contabilità e di finanza pubblica con la quale si è inteso razionalizzare e potenziare il complesso delle regole e delle procedure che presiedono il sistema delle decisioni di bilancio, aggiornandolo alla luce delle novità emerse in tema di governance economica europea e del nuovo assetto dei rapporti economici e finanziari tra lo Stato e le autonomie territoriali derivante dall'attuazione del federalismo fiscale.

- decreto legislativo 19 agosto 2016, n.175

Il decreto legislativo n.175 del 2016 reca il "Testo unico in materia di società a partecipazione pubblica".

- decreto legislativo 18 maggio 2018, n. 65.

Il decreto legislativo n. 65 del 2018 reca l'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 (Direttiva NIS).

- decreto legislativo 30 giugno 2003, n.196

Il decreto legislativo n.196 del 2003 reca il "Codice in materia di protezione dei dati personali".

- decreto legislativo 4 marzo 2014, n.39

Con il decreto legislativo n.39 del 2014 si è data attuazione nel nostro ordinamento alla direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI.

- legge 3 agosto 2007, n. 124

Con la legge n. 124 del 2007 è stato istituito, riformando il comparto dell'*intelligence* italiana, il sistema di informazione per la sicurezza della Repubblica ed è stata prevista la nuova disciplina in materia di segreto.

- decreto legislativo 10 agosto 2018, n.101

Il decreto legislativo n.101 del 2018 reca "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

- decreto-legge 27 luglio 2005, n.144

Il decreto-legge n.144 del 2005, reca "Misure urgenti per il contrasto del terrorismo internazionale" e, all'articolo 7-bis, reca disposizioni in merito all'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, individuato nel Servizio della polizia postale e delle comunicazioni.

- decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133

Il decreto-legge n. 105 del 2019 contiene disposizioni in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.

- legge 23 agosto 1988, n. 400

La legge n. 400 del 1988 reca la "Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri".

- legge 24 dicembre 2012, n.234

La legge n. 234 del 2012 disciplina il processo di partecipazione dell'Italia alla formazione delle decisioni e alla predisposizione degli atti dell'Unione europea e garantisce l'adempimento degli obblighi e l'esercizio dei poteri derivanti dall'appartenenza dell'Italia all'Unione europea, in coerenza con gli articoli 11 e 117 della Costituzione, sulla base dei principi di attribuzione, di

sussidiarietà, di proporzionalità, di leale collaborazione, di efficienza, di trasparenza e di partecipazione democratica.

- legge 28 dicembre 2015, n. 208

La legge n. 208 del 2015 reca le ª Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge di stabilità 2016)º .

3) ***Incidenza delle norme proposte sulle leggi e i regolamenti vigenti.***

Le disposizioni contenute nel decreto legislativo in esame incidono su talune disposizioni normative. In particolare, l' articolo 41 dispone l' abrogazione del D.Lgs. n. 65/2018 di recepimento della prima Direttiva NIS e degli articoli 40 (Sicurezza delle reti e dei servizi) e 41 (Attuazione e controllo) del D.Lgs. 259/2003 recante ª Codice europeo delle comunicazioni elettroniche º, prevedendo una fase transitoria fino all' emanazione dei provvedimenti attuativi del decreto.

Inoltre, l' articolo 43 introduce alcune modifiche alla disciplina nazionale in materia di sicurezza cibernetica in linea con quanto disposto dall' articolo 3, comma 1, lettera p), della legge di Delegazione europea 2022-2023 che prevede di ª *p) apportare alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il coordinamento con le disposizioni emanate in attuazione del presente articolo* º .

Nello specifico, sono previste alcune modifiche al decreto-legge 14 giugno 2021, n. 82, convertito con modificazione dalla legge 4 agosto 2021, n. 109, per assicurare la coerenza con l' architettura nazionale di cybersicurezza e i compiti dell' Agenzia per la cybersicurezza nazionale.

Sono previste, inoltre, modifiche al decreto-legge del 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge del 18 novembre 2019, n. 133, al fine di assicurare la coerenza con gli obblighi di cui al capo IV (obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente) e con le previsioni di cui al capo V (monitoraggio, vigilanza ed esecuzione) del decreto in esame.

4) ***Analisi della compatibilità dell'intervento con i principi costituzionali***

Non si rilevano profili di incompatibilità tra le misure contenute nel decreto legislativo con i principi costituzionali, con la giurisprudenza della Corte costituzionale, né con altre disposizioni vigenti.

5) ***Analisi delle compatibilità dell'intervento con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali.***

L' intervento è compatibile con le competenze e le funzioni delle regioni ordinarie e a statuto speciale nonché degli enti locali, rispetto alle quali sarà acquisito il prescritto parere della Conferenza unificata di cui all@rticolo 8 del decreto legislativo 28 agosto 1997, n. 281.

Inoltre, ai fini dell' attuazione del decreto, con accordo definito entro il 30 settembre 2024, in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, sono definite modalità di collaborazione tra le Autorità di settore e le regioni interessate, quando il soggetto importante e/o essenziale 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.

6) ***Verifica della compatibilità con i principi di sussidiarietà, differenziazione ed adeguatezza sanciti dall'articolo 118, primo comma, della Costituzione.***

Non si rilevano profili di incompatibilità con i principi di sussidiarietà, differenziazione e adeguatezza sanciti dall' articolo 118, primo comma, della Costituzione.

7) ***Verifica dell'assenza di rilegificazioni e della piena utilizzazione delle possibilità di delegificazione e degli strumenti di semplificazione normativa.***

Il provvedimento non comporta effetti di rilegificazione e non prevede l' utilizzo di strumenti di delegificazione e semplificazione normativa.

8) ***Verifica dell'esistenza di progetti di legge vertenti su materia analoga all'esame del Parlamento e relativo stato dell'iter.***

Risulta assegnato, in seconda lettura, al Senato della Repubblica l' AS 1143, già AC 1717, recante ª Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informaticiº . Attualmente, è in corso l' esame in Commissione - assegnato alle Commissioni riunite 1ã (Affari Costituzionali) e 2ã (Giustizia).

9) ***Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi di costituzionalità sul medesimo o analogo progetto.***

Non vi sono da segnalare indicazioni della giurisprudenza e non risultano pendenti giudizi di costituzionalità sull©ggetto del presente decreto.

PARTE II. CONTESTO NORMATIVO COMUNITARIO E INTERNAZIONALE

1) Analisi della compatibilità dell'intervento con l'ordinamento comunitario.

Il provvedimento in esame non presenta profili di incompatibilità con il diritto dell' Unione europea. Si tratta, invero, del decreto di recepimento della direttiva (UE) 2022/2555. La legge 21 febbraio 2024, n. 15 (Legge di delegazione europea 2022-2023) ha conferito (articolo 3) apposita delega legislativa al Governo, per il recepimento della suindicata direttiva, da esercitarsi nell' osservanza, oltreché dei principi e criteri direttivi generali di cui all' articolo 32 della legge 24 dicembre 2012, n.234, anche dei principi e criteri direttivi specifici ivi indicati.

2) Verifica dell'esistenza di procedure d'infrazione da parte della Commissione europea sul medesimo o analogo oggetto.

Attualmente non risultano procedure di infrazioni aperte sulla materia oggetto del decreto.

3) Analisi della compatibilità dell'intervento con* gli *obblighi internazionali.

Il decreto in esame non presenta profili di incompatibilità con obblighi internazionali.

4) ***Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte di Giustizia dell'Unione europea sul medesimo o analogo oggetto.***

Non vi sono da segnalare indicazioni della giurisprudenza e non risultano giudizi pendenti innanzi alla Corte di Giustizia vertenti sul medesimo o analogo oggetto.

5) Indicazioni delle linee prevalenti della giurisprudenza ovvero della pendenza di giudizi innanzi alla Corte europea dei diritti dell'uomo sul medesimo o analogo oggetto.

Non si è a conoscenza di linee prevalenti della giurisprudenza e non risultano giudizi pendenti innanzi alla Corte Europea dei Diritti dell' uomo.

6) Eventuali indicazioni sulle linee prevalenti della regolamentazione sul medesimo oggetto da parte di altri Stati membri dell'Unione europea.

Non vi sono indicazioni da segnalare in ordine alle linee prevalenti adottate sul medesimo oggetto da parte di altri Stati membri dell' Unione europea.

PARTE III. ELEMENTI DI QUALITÀ SISTEMATICA E REDAZIONALE DEL TESTO

1) ***Individuazione delle nuove definizioni normative introdotte dal testo, della loro necessità, della coerenza con quelle già in uso.***

Non vengono utilizzate definizioni normative che non appartengano già al linguaggio tecnico giuridico della materia regolata con le disposizioni contenute nel decreto legislativo in esame. Si è provveduto solamente, in alcuni casi, a chiarire e affinare definizioni già in uso nell' ordinamento italiano.

2) ***Verifica della correttezza dei riferimenti normativi contenuti nel progetto, con particolare riguardo alle successive modificazioni e integrazioni subite dai medesimi.***

È stata verificata positivamente la correttezza dei riferimenti normativi contenuti negli articoli del provvedimento.

3) ***Ricorso alla tecnica della novella legislativa per introdurre modificazioni ed integrazioni a disposizioni vigenti.***

Le disposizioni contenute nel decreto legislativo prevedono la modifica delle seguenti disposizioni vigenti.

Al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono apportate modificazioni (Articolo 43, comma 1):

- all' articolo 1, comma 1, lettera d);
- all' articolo 7, comma 1, lettera d);
- all' articolo 7, comma 1, lettera n);
- all' articolo 7, comma 1, lettera n-bis);
- all' articolo 7, comma 3;
- all' articolo 15.

Al decreto-legge del 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge del 18 novembre 2019, n. 133, sono apportate modificazioni (articolo 43, comma 2):

- all' articolo 1, comma 8;
- all' articolo 1, comma 3-bis;
- all' articolo 1, comma 17.

·***Individuazione di effetti abrogativi impliciti di disposizioni dell'atto normativo e loro traduzione in norme abrogative espresse nel testo normativo.***

Non si ravvisano effetti abrogativi impliciti nelle disposizioni contenute nel presente decreto legislativo.

4) ***Individuazione di disposizioni dell'atto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica o derogatorie rispetto alla normativa vigente.***

Non sussistono disposizioni dell@tto normativo aventi effetto retroattivo o di reviviscenza di norme precedentemente abrogate o di interpretazione autentica.

5) ***Verifica della presenza di deleghe aperte sul medesimo oggetto, anche a carattere integrativo o correttivo.***

L' articolo 3 della legge 21 febbraio 2024, n. 15 (Legge di delegazione europea 2022-2023) ha conferito apposita delega legislativa al Governo, per il recepimento della direttiva (UE) 2022/2555, da esercitarsi nell' osservanza, oltreché dei principi e criteri direttivi generali di cui all' articolo 32 della legge 24 dicembre 2012, n.234, anche dei principi e criteri direttivi specifici ivi indicati.

6) ***Indicazione degli eventuali atti successivi attuativi; verifica della congruenza dei termini previsti per la loro adozione.***

In attuazione delle misure contenute nel decreto legislativo in esame sono previsti diversi DPCM e determinazioni dell' Agenzia per la cybersicurezza nazionale, di seguito indicati:

● con uno o più decreti del Presidente del Consiglio dei ministri adottati, anche su proposta dei Ministri della giustizia, dell' interno e della difesa, per gli ambiti di rispettiva competenza, d' intesa con l' Agenzia per la cybersicurezza nazionale, sono individuati i soggetti che svolgono attività o forniscono servizi in via esclusiva per gli enti, organi e articolazioni della pubblica amministrazione di cui al comma 3 (Art. 4, comma 4);

● con decreto del Presidente del Consiglio dei ministri, adottato ai sensi dell' articolo 43 della legge 3 agosto 2007, n. 124, sono individuati i soggetti che svolgono attività o forniscono servizi in via esclusiva per gli Organismi di informazione per la sicurezza nazionale di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007 (Art. 4, comma 5);

● con uno o più decreti del Presidente del Consiglio dei ministri per la definizione del piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala (Art.13, comma 3).
Entro 12 mesi dall' entrata in vigore del decreto di recepimento, in esame.

● Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro della difesa, sentita l' Agenzia per la cybersicurezza nazionale, è definito, nell' ambito dell' elenco di cui all' articolo 7, comma 2, l' elenco dei soggetti che impattano sulla efficienza dello Strumento

militare e sulla tutela della difesa e sicurezza militare dello Stato, su cui l'Autorità nazionale competente NIS comunica tempestivamente al Ministero della difesa gli incidenti di cui all'articolo 25, nonché, con le modalità previste nel decreto di cui alla presente lettera, le ulteriori informazioni di sicurezza cibernetica (Art. 14, comma 2, lett. d);

● con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere del Comitato interministeriale per la cybersicurezza, adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, per:

- definire i criteri per l'applicazione della clausola di salvaguardia di cui all'articolo 3, comma 4
Entro 30 giorni dall'entrata in vigore del decreto di recepimento, in esame.

- stabilire i criteri, le procedure e le modalità di cui all'articolo 34, comma 10
Entro 6 mesi dall'entrata in vigore del decreto di recepimento, in esame.

- individuare le modalità di applicazione, nell'ambito del procedimento sanzionatorio, degli strumenti deflattivi del contenzioso di cui all'articolo 38, comma 15
Entro 6 mesi dall'entrata in vigore del decreto di recepimento, in esame.

● Con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale, d'intesa con le Autorità di settore NIS interessate, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere del Comitato interministeriale per la cybersicurezza, adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400:

- possono essere stabiliti ulteriori criteri di identificazione delle tipologie di soggetto di cui agli allegati III, nonché delle ulteriori tipologie di soggetto di cui all'articolo 3;

- possono essere individuate ulteriori categorie di pubbliche amministrazioni di cui all'articolo 3, commi 6 e 7 a cui si applica il presente decreto;

- sono stabilite le modalità di collaborazione tra l'Agenzia per la cybersicurezza nazionale e le Autorità di settore NIS ai fini del presente decreto ai sensi dell'articolo 11, comma 1;
Entro 6 mesi dall'entrata in vigore del decreto di recepimento, in esame.

● Con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale, d'intesa con le Amministrazioni interessate, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere del Comitato interministeriale per la cybersicurezza, adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, sono stabilite, ove necessario, le modalità di cooperazione e collaborazione di cui all'articolo 14, comma 5.

● Con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, su proposta delle Autorità di settore NIS interessate, sentito il Tavolo per l'attuazione della disciplina NIS una o più determinazioni dell'Agenzia per la cybersicurezza nazionale per:

- individuare, ove necessario, i soggetti ai quali si applica la clausola di salvaguarda di cui all'articolo 3, comma 4;

- individuare i soggetti ai quali si applica il presente decreto ai sensi dell'articolo 3, commi 8 e 9;
Entro 30 giorni dall'entrata in vigore del decreto di recepimento, in esame.

● Con una o più determinazioni dell' Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l' attuazione della disciplina NIS:

a) ai sensi degli articoli 3 e 6, è stabilito l' elenco dei soggetti essenziali e importanti di cui all' articolo 7, comma 2;

b) sono stabiliti i termini, le modalità nonché i procedimenti di utilizzo e accesso di cui all' articolo 7, comma 6, le eventuali ulteriori informazioni che i soggetti devono fornire ai sensi dei commi 1 e 4 del medesimo articolo nonché di designazione dei rappresentanti di cui all' articolo 5, comma 3
Entro 30 giorni dall' entrata in vigore del decreto di recepimento, in esame.

- definire l' organizzazione e il funzionamento del Tavolo per l' attuazione della disciplina NIS di cui all' articolo 12;
Entro 30 giorni dall' entrata in vigore del decreto di recepimento, in esame.

- adottare, d' intesa con il Ministero della giustizia, la politica nazionale di divulgazione coordinata delle vulnerabilità di cui all' articolo 16, comma 4;
Entro 6 mesi dall' entrata in vigore del decreto di recepimento, in esame.

- possono essere imposte condizioni per le informazioni messe a disposizione dalle autorità competenti e dal CSIRT Italia nel contesto degli accordi di condivisione delle informazioni sulla sicurezza informatica di cui all' articolo 17, comma 3;

- stabilire le modalità con cui i soggetti essenziali e importanti notificano all' Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione delle informazioni sulla sicurezza informatica di cui all' articolo 17, comma 4;

- stabilire obblighi proporzionati e graduali, a valenza multisettoriale e, ove opportuno, settoriale, di cui all' articolo 31, le modalità di applicazione dei medesimi obblighi per i soggetti che svolgono attività in più settori o sottosettori e per i soggetti di cui all' articolo 32, commi 1 e 2;
Entro 6 mesi dall' entrata in vigore del decreto di recepimento, in esame.

- possono essere designati gli esperti di sicurezza informatica di cui all' articolo 21, comma 1, nonché individuate, se necessario, le modalità per l' esecuzione della revisione tra pari di cui al medesimo articolo, commi 2 e 3;

- può essere imposto l' utilizzo di prodotti TIC, servizi TIC e processi TIC certificati di cui all' articolo 27, definito i relativi termini, criteri e modalità;

- stabilire le categorie di rilevanza nonché le modalità e i criteri per l' elencazione, caratterizzazione e categorizzazione delle attività e dei servizi, a valenza multisettoriale e, ove opportuno, settoriale, di cui all' articolo 30;
Entro 18 mesi dall' entrata in vigore del decreto di recepimento, in esame.

- possono essere specificati, laddove necessario, i criteri per la determinazione dell' importo delle sanzioni ai sensi dell' articolo 38, comma 2.

7) ***Verifica della piena utilizzazione e dell'aggiornamento di dati e di riferimenti statistici attinenti alla materia oggetto del provvedimento, ovvero indicazione della necessità di***

commissionare all'Istituto nazionale di statistica apposite elaborazioni statistiche con correlata indicazione nella relazione economico-finanziaria della sostenibilità dei relativi costi.

Per la predisposizione del provvedimento in esame sono stati utilizzati i dati informativi già in possesso dell' Amministrazione proponente e non è stato necessario commissionare l' acquisizione di ulteriori dati statistici o informativi.

ANALISI DELL'IMPATTO DELLA REGOLAMENTAZIONE (A.I.R.)

(Allegato 2 della direttiva del P.C.M. in data 16 febbraio 2018 ± G.U. 10 aprile 2018, n. 83)

Provvedimento: Schema di decreto legislativo di recepimento della direttiva (UE) 2022/2555, 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.

Amministrazione competente: Presidenza del Consiglio dei ministri ± Agenzia per la cybersicurezza nazionale

Referente: Presidenza del Consiglio dei ministri

SINTESI DELL'AIR E PRINCIPALI CONCLUSIONI

Con la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio (cosiddetta direttiva NIS) il legislatore europeo ha posto le basi per sviluppare le capacità di cybersicurezza in tutta l'Unione al fine di mitigare le minacce ai sistemi informativi e di rete utilizzati per fornire servizi essenziali in settori chiave e garantire la continuità di tali servizi in caso di incidenti, contribuendo in tal modo alla sicurezza dell'Unione e al funzionamento efficace della sua economia e della sua società. Tale direttiva ha garantito il completamento dei quadri nazionali, definendo le rispettive strategie sulla sicurezza dei sistemi informativi e di rete, stabilendo capacità nazionali, nonché attuando misure normative riguardanti le infrastrutture e gli attori essenziali individuati da ciascuno Stato membro. La direttiva (UE) 2016/1148 ha, inoltre, contribuito alla cooperazione a livello dell'Unione mediante l'istituzione del gruppo di cooperazione e della rete di gruppi nazionali di intervento per la sicurezza informatica in caso di incidente.

Tuttavia, nonostante tali risultati, l'applicazione della direttiva NIS ha rivelato carenze intrinseche che costituiscono un limite alla capacità di affrontare efficacemente le sfide attuali ed emergenti in materia di cybersicurezza.

Con la direttiva (UE) 2022/2555 (cosiddetta direttiva NIS 2) del Parlamento europeo e del Consiglio del 14 dicembre 2022, viene abrogata la direttiva NIS e vengono poste in essere misure per superare tali carenze.

La direttiva NIS 2 fa parte di un pacchetto ampio di strumenti giuridici e di iniziative a livello dell'Unione, mirato ad aumentare la resilienza di soggetti pubblici e privati alle minacce nell'ambito cibernetico; tra le disposizioni più recenti del pacchetto si segnalano il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario (cosiddetto regolamento DORA - *Digital Operational Resilience Act*) e la correlata direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, sempre relativa alla resilienza operativa digitale per il settore finanziario, nonché la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici (cosiddetta direttiva CER ± *Critical Entities Resilience*). Tra i richiamati atti e la direttiva NIS 2, vi è una importante contiguità applicativa dimostrata anche dalla pubblicazione degli stessi nella medesima edizione della GUUE.

Il nuovo impianto posto in essere dalla direttiva NIS 2, dunque, supera e rafforza quanto già previsto dalla precedente direttiva NIS, recepita nell'ordinamento nazionale con il decreto legislativo 18 maggio 2018, n. 65 (decreto legislativo NIS), in particolare attraverso:

1) l'ampliamento del campo di applicazione, includendo 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, con un aumento significativo dei settori vigilati e l'introduzione di un approccio «*all-hazards*» alla cybersicurezza, che prevede l'inclusione di profili di sicurezza fisica delle infrastrutture ICT (*Information and Communications Technology*);

2) la revisione del meccanismo di identificazione dei soggetti quali entità importati o essenziali, prevedendo un criterio omogeneo basato sulla dimensione (cosiddetto *size-cap rule*), che estende l'applicazione della direttiva a tutte le medie e grandi imprese che operano nei settori identificati. Ciò al fine di superare l'attuale disomogeneità nel processo di identificazione dei soggetti da parte degli Stati membri;

3) il rafforzamento dei poteri di supervisione, con indicazioni più dettagliate per la definizione delle misure di sicurezza e l'inasprimento delle sanzioni;

4) l'ampliamento delle funzioni dei CSIRT (*Computer Security Incident Response Team*) nazionali, che fungeranno, tra l'altro, da intermediari di fiducia tra i soggetti segnalanti e i fornitori di prodotti e servizi ICT nell'ambito del quadro per la divulgazione coordinata delle vulnerabilità (*Coordinated Vulnerability Disclosure* – CVD);

5) la gestione delle crisi, con la previsione di una strategia in materia e l'istituzionalizzazione della *Cyber Crises Liaison Organisation Network* (CyCLONe), per la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala.

Nella redazione dello schema di decreto legislativo di recepimento, nel tenere conto dei criteri e dei principi direttivi di delega, contenuti nell'articolo 3 della legge 21 febbraio 2024, n. 15 (Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea - Legge di delegazione europea 2022-2023), riportati più avanti in maniera puntale nella sezione 3, si è anche deciso di operare, seppur in maniera limitata e laddove strettamente necessario, una redistribuzione dei contenuti della Direttiva, al fine di dotare il testo di una organicità complessiva e tenendo anche conto della posizione italiana espressa nella fase ascendente in sede di negoziato. In ragione di tale impostazione lo schema di decreto legislativo è strutturato nei seguenti Capi:

- **Capo I** – Disposizioni generali;
- **Capo II** – Quadro nazionale di sicurezza informatica;
- **Capo III** – Cooperazione a livello dell'Unione europea e internazionale;
- **Capo IV** – Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente;
- **Capo V** – Monitoraggio, vigilanza ed esecuzione;
- **Capo VI** – Disposizioni finali e transitorie.

1. CONTESTO E PROBLEMI DA AFFRONTARE

A livello europeo, l'esigenza di aumentare la resilienza cibernetica discende dalla necessità di modernizzare il quadro giuridico esistente alla luce della crescente digitalizzazione del mercato interno e della rapida evoluzione delle minacce alla cybersicurezza, conseguentemente revisionando, al predetto fine, la direttiva NIS. Inoltre, un'analisi del funzionamento della direttiva NIS, condotta ai fini della valutazione d'impatto che ha accompagnato la proposta di direttiva NIS 2 (COM (2020) 823 *final*, del 16 dicembre 2020) ha identificato i seguenti problemi:
- un ambito di applicazione eccessivamente limitato in termini di settori considerati, principalmente a causa dell'aumento della digitalizzazione negli ultimi anni, con conseguente impossibilità da parte della direttiva NIS di riflettere tutti i settori digitalizzati che forniscono servizi chiave all'economia e alla società nel suo complesso;
- un'ambiguità relativamente all'ambito di applicazione per gli operatori di servizi essenziali e relativamente alle competenze nazionali sui fornitori di servizi digitali, che comporta che taluni soggetti non siano individuati come tali in tutti gli Stati membri e non abbiano, pertanto, l'obbligo di mettere in atto misure di sicurezza e segnalare incidenti;
- un'ampia discrezionalità nello stabilire i requisiti di sicurezza e di segnalazione di incidenti per gli operatori di servizi essenziali, che determina, in taluni casi, un'adozione eccessivamente diversificata tra gli Stati membri di tali requisiti e crea oneri aggiuntivi per le società operanti in più di uno Stato membro;
- la sussistenza di divergenze nell'attuazione delle disposizioni in materia di vigilanza ed esecuzione della direttiva NIS, che comporta una frammentazione del mercato interno con ripercussioni, in particolare, sulla fornitura transfrontaliera di servizi e sul livello di cyber resilienza e sulla vulnerabilità di taluni Stati membri di fronte alle minacce informatiche, con potenziali ricadute sull'intera Unione;
- un'eccessiva eterogeneità relativamente alle risorse finanziarie e umane previste dagli Stati membri per l'adempimento dei loro compiti (come l'identificazione o la vigilanza degli operatori di servizi essenziali), che comporta un'eterogeneità di capacità nell'affrontare i rischi di cybersicurezza;
- uno scarso livello di condivisione tra gli Stati membri delle informazioni, con conseguenze negative in particolare sull'efficacia delle misure di cybersicurezza e sul livello di consapevolezza situazionale comune a livello dell'UE. Lo stesso può dirsi anche per la condivisione di informazioni tra soggetti privati e per il coinvolgimento tra soggetti privati e strutture di cooperazione a livello dell'UE.

A livello nazionale, il contesto geopolitico, influenzato dai conflitti in Ucraina e in Medio Oriente, è caratterizzato dall'aumento di azioni cyber malevoli, principalmente eventi di tipo DDoS[1] a danno di siti *web* di pubbliche amministrazioni e imprese e, in numero esiguo, di tipo *defacement*, ossia intrusioni informatiche che consistono nel modificare pagine di siti *web* sostituendole con un messaggio di rivendicazione, di apologia e simili. Per quanto riguarda i soggetti interessati da DDoS nel 2023, questi sono stati principalmente pubbliche amministrazioni centrali e aziende del settore dei trasporti e dei servizi finanziari.
In tale contesto, l'Agenzia per la cybersicurezza nazionale - istituita con il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni dalla legge 4 agosto 2021, n. 109, con il compito tutelare la sicurezza e la resilienza nello spazio cibernetico - ha rafforzato il proprio impegno per garantire la diffusione di informazioni sui rischi cyber oltre che per fornire assistenza alle vittime.

1 Gli eventi DDoS (*Distributed Denial of Service*) mirano a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria. L'effetto più immediato di tale tipologia di attacco è l'indisponibilità del sito o del servizio colpito.

L'Agenzia, attraverso il CSIRT Italia (organo dell'Agenzia che si occupa di monitoraggio preventivo e risposta agli incidenti informatici) ha potuto monitorare l'evoluzione della minaccia, caratterizzata sempre più da eventi di tipo *ransomware* e DDoS ± ma anche diffusione di *malware*[2] via *e-mail* e *phishing*[3] ± e indirizzata a diverse realtà pubbliche oltre che ad aziende attive nei settori più disparati (primi fra tutti telecomunicazioni, trasporti e servizi finanziari).
Al riguardo, il CSIRT Italia effettua campagne di allertamento per i soggetti obiettivo dei DDoS, indicando loro contromisure di mitigazione specifiche per gli attacchi in corso, oltre a pubblicare sul proprio portale pubblico bollettini dedicati. Svolge, inoltre, numerose attività di sensibilizzazione al fine di elevare il livello di allerta degli operatori pubblici e privati su potenziali effetti di *spillover* di incidenti, ovvero infezioni di soggetti operanti sui territori coinvolti nei conflitti e con i quali aziende italiane condividono reti e sistemi.
Un'altra minaccia in aumento è costituita dagli attacchi *ransomware*, ossia, operazioni tramite le quali l'attaccante, di regola, si introduce nei sistemi di un soggetto per cifrarne i dati, al fine di ottenere il pagamento di un riscatto necessario a rendere le informazioni nuovamente disponibili al legittimo proprietario e/o a non diffonderle pubblicamente.
Nel 2023, la minaccia *ransomware* si è confermata come quella più significativa, soprattutto alla luce dell'impatto che ha avuto a livello nazionale, con 165 eventi diretti verso operatori privati e pubbliche amministrazioni, e un incremento del 27 % rispetto al 2022.
È da ritenere, tuttavia, che il dato rappresenti solo una parte del numero complessivo di attacchi *ransomware* effettivamente avvenuti, tenuto conto che le vittime, spesso sprovviste di *know-how* e strutture interne dedicate ± in particolare le piccole e medie imprese (PMI) ± talvolta non segnalano l'evento. Nella grande maggioranza dei casi (84%) le vittime di attacchi *ransomware* appartengono al settore privato. Per quanto attiene alla dimensione aziendale dei soggetti privati colpiti, circa il 23% degli eventi *ransomware* ha interessato grandi imprese, mentre in oltre il 75% dei casi sono state coinvolte piccole (46,3%) e medie imprese (30,6%).
Nel contesto nazionale sopra illustrato, dunque, l'attuazione della direttiva NIS 2 appare indispensabile per promuovere l'utilizzo di reti e sistemi sicuri, specialmente quando funzionali all'operatività delle infrastrutture cruciali per la tenuta del Sistema Paese, e mitigare le criticità che, come richiamato, sono state rilevate anche in ambito nazionale, con particolare riguardo alla ristrettezza dell'ambito di applicazione e all'ambiguità sulla individuazione dei soggetti cui rivolgere le misure di sicurezza e gli obblighi previsti dalla direttiva NIS.
Quanto all'ambito di applicazione, lo schema di decreto legislativo ne prevede l'ampliamento includendo anche le pubbliche amministrazioni ricomprese nelle rispettive categorie di cui agli allegati III e IV del medesimo decreto. Il decreto legislativo, nel distinguere i settori ritenuti, rispettivamente, altamente critici e critici, al fine di superare l'attuale disomogeneità nel processo di identificazione dei soggetti da parte degli SM, introduce il criterio di individuazione dei soggetti su base dimensionale (cd. *Size-cap rule*), estendendo l'applicazione della NIS2 a tutte le medie e grandi imprese che operano nei settori di cui agli allegati I e II. Sono altresì sottoposti al presente schema di decreto legislativo, indipendentemente dalla loro dimensione, i soggetti ai quali si applica la direttiva CER; i fornitori di reti pubbliche di comunicazione elettroniche o di servizi di comunicazione elettronica accessibili al pubblico; i prestatori di servizi fiduciari; i gestori di

2 Programma inserito in un sistema informatico, generalmente in modo abusivo e occulto, con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

3 Attacco informatico avente, generalmente, l'obiettivo di carpire informazioni sensibili (*user ID, password*, numeri di carte di credito, PIN) con l'invio di false e-mail generiche a un gran numero di indirizzi. Le e-mail sono congegnate per convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. L'attaccante utilizza i dati carpiti per acquistare beni, trasferire somme di denaro o anche solo come ª ponteº per ulteriori attacchi.

registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio; i fornitori di servizi di registrazione dei nomi di dominio.
Gli operatori di servizi essenziali o importanti dovranno notificare al CSIRT Italia, senza indebito ritardo e non oltre 72 ore dalla venuta a conoscenza tutti quegli incidenti in grado di causare una grave perturbazione del servizio oppure se l'incidente può avere conseguenze (o ha già avuto conseguenze) su altre persone fisiche o giuridiche causando perdite considerevoli. In aggiunta sono previste notifiche al CSIRT Italia su base volontaria:
- degli incidenti, ovvero un evento che comprometta 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;
- delle minacce informatiche, ovvero 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;
- dei quasi incidenti, ovvero qualsiasi evento che avrebbe potuto compromettere 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, ma che è stato efficacemente evitato o non si è verificato.
Lo schema di decreto legislativo ha, inoltre, esteso la definizione di incidente includendovi anche quelli capaci di compromette la ª disponibilitàº, la ª autenticitàº, la ª integritàº o la ª riservatezzaº di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi, non limitandosi, dunque, solo a quelli che hanno un impatto rilevante sulla ª continuitàº dei servizi essenziali prestati.
In relazione a tanto sono, dunque, stati previsti gli specifici criteri di delega di cui alle lettere d) ed e), del richiamato articolo 3 della legge n. 15 del 2024, e declinati nello schema di decreto legislativo con la finalità di confermare l'architettura delineata dal decreto-legge n. 82 del 2021.
In questo senso il decreto legislativo prevede, infatti, la conferma dell'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS, Punto di contatto unico NIS e Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente (CSIRT Italia) in ambito nazionale, e la designa anche quale Autorità competente alla gestione degli incidenti e delle crisi informatiche su vasta scala (Autorità di gestione delle crisi informatiche), di cui all'articolo 9 della direttiva, con funzioni di coordinatore ai sensi del paragrafo 2, del medesimo articolo 9, insieme al Ministero della difesa, ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera g), del presente decreto. Vengono, inoltre, individuate le Autorità di settore NIS a completamento di una *governance* nazionale che viene ridisegnata nell'ottica di un deciso miglioramento e rafforzamento rispetto al sistema precedentemente prevista per l'attuazione della NIS.
Rispetto alle misure di sicurezza, lo schema di decreto legislativo prevede che l'Autorità competente NIS possa imporre ai soggetti essenziali e importanti l'utilizzo di determinati prodotti TIC (un elemento o un gruppo di elementi di un sistema informativo o di rete), servizi TIC (un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo dei sistemi informativi e di rete) e processi TIC (un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC), sviluppati dal soggetto essenziale o importante o acquistati da terze parti, purché siano certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza. Si attribuisce alla stessa Autorità la facoltà di promuovere l'uso di specifiche tecniche per favorire l'attuazione efficace e armonizzata delle misure di gestione dei rischi di sicurezza cibernetica, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia.

2. OBIETTIVI DELL'INTERVENTO E RELATIVI INDICATORI

2.1 Obiettivi generali e specifici

Gli obiettivi generali perseguiti dallo schema di decreto legislativo sono:

- un aumento del livello di cyber resilienza del Paese sia per i soggetti pubblici e sia per i soggetti privati operanti in ambito nazionale in tutti i settori pertinenti;

- la riduzione delle incongruenze, in termini di resilienza, nei settori contemplati dal decreto legislativo;

- miglioramento del livello di consapevolezza situazionale comune e la capacità di preparazione e risposta alle crisi.

Gli obiettivi specifici si prefiggono di raggiungere gli obiettivi generali e consistono, dunque:

- nell'aggiornamento delle misure per un comune livello elevato di cybersicurezza nell'ordinamento interno, rivolte sia ai soggetti pubblici e sia a quelli privati che operano in ambito nazionale nei settori ricompresi dall'applicazione del decreto legislativo, che utilizzano sistemi informativi e di rete e che forniscono servizi chiave all'economia e alla società nel suo complesso, in maniera che tali soggetti siano tenuti ad adottare misure adeguate di cybersicurezza e a segnalare gli incidenti, anche attraverso un significativo ampliamento dei settori vigilati e un rafforzamento delle misure di gestione dei rischi di cybersicurezza;

- quanto al problema del livello incoerente di resilienza tra i settori, nel garantire che tutti i soggetti attivi in settori disciplinati dal quadro giuridico del decreto legislativo, di dimensioni simili e aventi un ruolo comparabile, siano soggetti allo stesso regime di disciplina. Una corretta postura cyber del «sistema Paese» rende il contesto istituzionale pubblico e il tessuto produttivo nazionale non solo più sicuri ma con riferimento al mondo imprenditoriale anche più affidabile e competitivo a livello europeo e internazionale;

- quanto al problema della consapevolezza situazionale comune e della mancanza di una risposta efficace alle crisi, nel garantire lo scambio di informazioni essenziali tra i diversi soggetti previsti dalla governance nazionale, con l'introduzione di obblighi di condivisione di informazioni e di cooperazione chiari tra le diverse autorità competenti in relazione a minacce e incidenti informatici e sviluppando una capacità operativa comune di risposta alle crisi. L'attuale contesto geo-politico, infatti, caratterizzato in particolare dai gravi conflitti internazionale in atto, favorisce l'incremento delle minacce informatiche e richiede, pertanto, in modo sempre più incalzante, il raggiungimento di un alto livello di cybersicurezza, attraverso l'attuazione di efficaci misure di gestione dei relativi rischi, nonché la necessità di un'immediata e quanto più completa conoscenza situazionale.

2.2 Indicatori e valori di riferimento

Gli indicatori che, monitorati nel tempo, potranno consentire di valutare il grado di raggiungimento degli obiettivi dell'intervento normativo possono essere riassunti nel seguente elenco, non esaustivo:

· migliore gestione degli incidenti

Adottando misure di cybersicurezza, le pubbliche amministrazioni e le imprese non migliorano soltanto la propria capacità di evitare completamente determinati incidenti, ma anche la capacità di risposta. Gli esiti positivi sono quindi misurati in base:

a) alla riduzione del tempo medio necessario per rilevare un incidente;

b) al tempo mediamente necessario alle organizzazioni per riprendersi da un incidente;

c) al costo medio di un danno causato da un incidente;

· maggiore consapevolezza dei rischi di cybersicurezza

Questo aspetto può essere misurato analizzando fino a che punto i soggetti pubblici e privati rientranti nell'ambito di applicazione della NIS 2 diano priorità alla cybersicurezza nelle politiche e nei processi interni, come dimostrato dalla documentazione interna, dai programmi di formazione pertinenti e dalle attività di sensibilizzazione per i dipendenti, e agli investimenti in TIC correlati alla sicurezza. Il management dei soggetti essenziali e importanti dovrebbero essere anche a conoscenza delle norme stabilite dalla direttiva NIS 2;

· livellamento della spesa specifica per settore

La spesa per la sicurezza delle TIC varia notevolmente tra i diversi settori. Obbligando le imprese di più settori ad adottare misure di un certo tipo, si dovrebbe assistere a una riduzione delle deviazioni dalla spesa media per la sicurezza delle TIC specifica per settore in percentuale della spesa complessiva per le TIC;

· governance più forti e maggiore cooperazione

Questo dovrebbe avere un'incidenza misurabile sulle risorse finanziarie e umane destinate ai soggetti della governance a livello nazionale e dovrebbe avere un impatto positivo sulla capacità di cooperare in modo proattivo tra i medesimi soggetti;

· maggiore condivisione delle informazioni

Il decreto legislativo si propone di migliorare anche la condivisione delle informazioni tra i soggetti pubblici, le imprese, l'autorità competente e quelle di settore e aumentare il numero di soggetti che partecipano alle varie forme di condivisione delle informazioni.

3. OPZIONI DI INTERVENTO E VALUTAZIONE PRELIMINARE

Lo schema di decreto legislativo è giustificato principalmente dai seguenti fattori: a) la natura sempre più transfrontaliera delle minacce e delle sfide legate alla NIS; b) le potenzialità degli interventi dell'Unione volti a migliorare e agevolare strategie nazionali efficaci e coordinate; e c) il contributo degli interventi strategici concertati e collaborativi volti a un'efficace protezione dei dati e della vita privata.

Lo strumento giuridico che è stato scelto a livello unionale è la direttiva, in quanto si tratta dello strumento che consente una migliore armonizzazione mirata, nonché un certo livello di flessibilità per le autorità competenti.

La resilienza in termini di cybersicurezza all'interno dell'Unione non può, infatti, essere efficace se affrontata in modo non uniforme tra i vari Stati membri. La direttiva NIS ha parzialmente ovviato a questa carenza definendo un quadro per la sicurezza delle reti e dei sistemi informativi a livello nazionale e dell'Unione. Tuttavia, il suo recepimento e la sua attuazione hanno portato alla luce carenze e limiti intrinseci di alcune disposizioni o approcci, come la poco chiara delimitazione del suo ambito di applicazione, che ha determinato differenze significative in termini di portata e intensità dell'intervento effettivo dell'UE a livello di Stati membri. Inoltre, con la crisi COVID-19, l'economia europea è diventata dipendente dai sistemi informatici e di rete come mai prima d'ora, mentre settori e servizi sono sempre più interconnessi.

Le opzioni di non intervento comporterebbero la mancata adozione di misure per affrontare le criticità rilevate nella valutazione della direttiva NIS e, pertanto, non vi sarebbe alcun cambiamento a livello legislativo.

Tanto premesso, anche in considerazione del fatto che la direttiva prevede l'obbligo per gli Stati membri di adottare le disposizioni legislative, regolamentari e amministrative necessarie per il recepimento della direttiva NIS 2, informandone la Commissione, non sono state prese in considerazione opzioni alternative all'intervento legislativo in esame.

Al fine di consentire il miglior adeguamento dell'ordinamento interno alle disposizioni della direttiva NIS 2 e superare le su richiamate criticità relative alla NIS, la delega è stata esercitata con la predisposizione dello schema di decreto legislativo in analisi osservando i seguenti ulteriori princìpi e criteri direttivi specifici oltre ai princìpi e criteri direttivi generali previsti dall'articolo 32 della legge 24 dicembre 2012, n. 234, che consentono di esercitare le opzioni principali indicate dalla Direttiva stessa.

Con la legge del 21 febbraio 2024, n. 15, recante «*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2022-2023*» e, in particolare con il citato articolo 3, è stata dettata la delega legislativa, corredata di specifici criteri, necessaria per il corretto recepimento della direttiva NIS 2 nell'ordinamento interno, prevedendo che:

«1. *Nell'esercizio della delega per il recepimento della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, il Governo, sentita l'Agenzia per la cybersicurezza nazionale, osserva, oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti princìpi e criteri direttivi specifici:*

a) 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, anche considerando la possibilità di applicazione della direttiva medesima ai comuni e alle province secondo princìpi di gradualità, proporzionalità e adeguatezza; b) escludere dall'ambito di applicazione delle disposizioni della direttiva (UE) 2022/2555 gli enti della pubblica amministrazione operanti nei settori di cui all'articolo 2, paragrafo 7, della direttiva medesima, compresi gli organismi di informazione per la sicurezza ai quali si applicano le disposizioni della legge 3 agosto 2007, n. 124;

b) avvalersi della facoltà di cui all'articolo 2, paragrafo 8, della direttiva (UE) 2022/2555, prevedendo che con uno o più decreti del Presidente del Consiglio dei ministri, adottati su proposta delle competenti amministrazioni, siano esentati soggetti specifici che svolgono attività nei settori ivi indicati o che forniscono servizi esclusivamente agli enti della pubblica amministrazione di cui all'articolo 2, paragrafo 7, della medesima direttiva;

c) escludere dall'ambito di applicazione delle disposizioni della direttiva (UE) 2022/2555 gli enti della pubblica amministrazione operanti nei settori di cui all'articolo 2, paragrafo 7, della direttiva medesima, compresi gli organismi di informazione per la sicurezza ai quali si applicano le disposizioni della legge 3 agosto 2007, n. 124;

d) confermare la distinzione tra l'Agenzia per la cybersicurezza nazionale, quale autorità nazionale competente e punto di contatto, ai sensi dell'articolo 8 della direttiva (UE) 2022/2555, e le autorità di settore operanti negli ambiti di cui agli allegati I e II alla medesima direttiva;

e) in relazione all'istituzione del team di risposta agli incidenti di sicurezza informatica (CSIRT), di cui all'articolo 10 della direttiva (UE) 2022/2555, 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;

f) prevedere un regime transitorio per i soggetti già sottoposti alla disciplina del decreto legislativo 18 maggio 2018, n. 65, recante attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, garantendo termini congrui di adeguamento, ai fini della migliore applicazione delle disposizioni previste dalla direttiva (UE) 2022/2555;

g) prevedere meccanismi che consentano la registrazione dei soggetti essenziali e importanti, di cui all'articolo 3 della direttiva (UE) 2022/2555, per la comunicazione dei dati previsti dal paragrafo 4 del medesimo articolo 3, compresi i soggetti che gestiscono servizi connessi o strumentali alle attività oggetto delle disposizioni della direttiva medesima relative al settore della cultura;

h) in relazione alle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555, prevedere 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 provvede altresì all'aggiornamento degli strumenti adottati;

i) introdurre nella legislazione vigente, anche in materia penale, le modifiche necessarie al fine di assicurare il corretto recepimento nell'ordinamento nazionale delle disposizioni della direttiva (UE) 2022/2555 in materia di divulgazione coordinata delle vulnerabilità; si suddivide in 6 Capi e 45 articoli, riproponendo la struttura della Direttiva NIS2 alla luce dei principi e dei criteri direttivi introdotti dall'articolo 3 della legge di Delegazione europea 2022-2023.

l) 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 del Parlamento europeo e del Consiglio, del 23 luglio 2014;

m) individuare criteri oggettivi e proporzionati ai fini dell'applicazione degli obblighi informativi di cui all'articolo 23, paragrafo 2, della direttiva (UE) 2022/2555;

n) rivedere il sistema sanzionatorio e il sistema di vigilanza ed esecuzione, in particolare:

1) prevedendo sanzioni effettive, proporzionate e dissuasive rispetto alla gravità della violazione degli obblighi derivanti dalla direttiva (UE) 2022/2555, anche in deroga ai criteri e ai limiti previsti dall'articolo 32, comma 1, lettera d), della legge 24 dicembre 2012, n. 234, e alla legge 24 novembre 1981, n. 689, introducendo strumenti deflativi del contenzioso, quali la diffida ad adempiere;

2) prevedendo che gli introiti derivanti dall'irrogazione delle sanzioni siano 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, di cui all'articolo 18 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale;

o) 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;

p) apportare alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il coordinamento con le disposizioni emanate in attuazione del presente articolo.º

Anche in coerenza con la delega conferita, nel decreto legislativo di recepimento, il legislatore delegato ha esercitato il proprio margine di discrezionalità, che la direttiva ha riservato agli Stati membri ai fini del recepimento negli ordinamenti nazionali. In particolare:

- con riferimento all'articolo 3, comma 1, lettera a), in relazione all'articolo 2, paragrafo 2, della direttiva NIS 2, sono stati indicati i criteri in base ai quali un ente pubblico può essere considerato pubblica amministrazione ai fini dell'applicazione delle disposizioni della direttiva medesima, anche considerando la possibilità di applicazione ai comuni e alle province secondo princìpi di gradualità, proporzionalità e adeguatezza. La scelta operata nel decreto legislativo, in linea con l'indicazione della delega, ha l'obiettivo di potenziare la resilienza cyber delle pubbliche amministrazioni, in quanto fattore chiave per la trasformazione digitale sicura e resiliente del Paese. Nel corso del 2023, infatti, sono stati registrati 422 eventi cyber ai danni di istituzioni pubbliche nazionali; dato in sensibile aumento rispetto ai 160 del 2022. Di questi eventi, 85 sono stati classificati come incidenti (nel 2022 furono 57), procurando nella maggior parte dei casi il malfunzionamento dei sistemi e conseguenti blocchi o rallentamenti nell'erogazione dei servizi;

- con riferimento all'articolo 3, comma 1, lettere b) e c), in relazione all'articolo 2, paragrafi 7 e 8, della Direttiva, si è scelto di esentare dall'ambito di applicazione del decreto gli enti della pubblica amministrazione 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, nonché soggetti specifici che svolgono attività, o che forniscono servizi esclusivamente agli enti della pubblica amministrazione, nei predetti settori;

- con riferimento all'articolo 3, comma 1, lettere d) ed e), in attuazione degli articoli 8 e 10 della direttiva NIS 2, l'Agenzia per la cybersicurezza nazionale è stata confermata quale «autorità competente», «punto di contatto unico», nonché quale «*Team* di risposta agli incidenti di sicurezza informatica (CSIRT)». Tale scelta è stata operata per mantenere l'architettura istituzionale delineata dal decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109. Quanto alla individuazione dell'autorità nazionale competente, infatti, la disciplina NIS, recata dal decreto legislativo n. 65 del 2018, prevedeva un sistema plurale di autorità competenti per settori (i Ministeri interessati) ed indicava il Dipartimento delle informazioni per la sicurezza quale punto di contatto. La nuova disciplina, invece ha posto, sopra le autorità di settore, una istanza di raccordo individuata nell'Agenzia per la cybersicurezza nazionale che ha assunto, dunque, il ruolo di Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto.

Sempre ai sensi del richiamato decreto-legge n. 82 del 2021, il CSIRT italiano di cui all'articolo 8 del decreto legislativo NIS è stato trasferito presso l'Agenzia e ha assunto la denominazione di «CSIRT Italia».

- con riferimento all'articolo 3, comma 1, lettera n), in relazione all'articolo 36 della direttiva NIS 2, , sono stati adeguati il sistema sanzionatorio e il sistema di vigilanza ed esecuzione prevedendo sanzioni effettive, proporzionate e dissuasive rispetto alla gravità della violazione degli obblighi derivanti dalla nuova Direttiva, anche in deroga ai criteri e ai limiti previsti dall'articolo 32, comma 1, lettera d), della legge 24 dicembre 2012, n. 234 e alla legge 24 novembre 1981, n. 689, introducendo altresì strumenti deflattivi del contenzioso, quali la diffida ad adempiere, l'invito a conformarsi alle decisioni dall'Autorità nazionale competente NIS e la facoltà di estinguere il procedimento attraverso il pagamento in misura ridotta.

Inoltre, sempre in relazione al principio di delega di cui alla richiamata lettera n) e alla necessità di migliorare e aumentare la condivisione di informazioni tra soggetti privati, nonché per il

coinvolgimento tra soggetti privati e strutture di cooperazione a livello nazionale e UE, è stata introdotta nell'ordinamento nazionale una specifica disciplina sulla divulgazione coordinata delle vulnerabilità (un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica) che attribuisce al CSIRT Italia il ruolo di coordinatore dei soggetti interessati 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, e prevede che sia adottata una politica nazionale di divulgazione coordinata delle vulnerabilità in linea con le previsioni del decreto e tenuto conto degli orientamenti del gruppo di cooperazione NIS.

Le scelte adottate dal legislatore europeo, ma anche le estensioni decise, sono realizzabili da un punto di vista legislativo e non presentano svantaggi.

La disciplina attualmente in vigore è affidata al decreto legislativo 18 maggio 2018, n. 65, con il quale è stata recepita in Italia la direttiva NIS, che lo schema di decreto legislativo in analisi provvede ad abrogare, prevedendo un periodo transitorio per garantire un'applicazione e un passaggio graduale tra il vecchio e il nuovo regime.

4. COMPARAZIONE DELLE OPZIONI E MOTIVAZIONE DELL'OPZIONE PREFERITA

4.1 Impatti economici, sociali e ambientali per categoria di destinatari

Si illustrano i risultati della comparazione delle opzioni attuabili:

- principali impatti (benefici e costi attesi) per ciascuna categoria di destinatari di cui alla sezione 1;

La direttiva NIS 2 e il presente intervento legislativo per la sua attuazione hanno la finalità di razionalizzare ulteriormente gli obblighi imposti alle imprese e promuovere un livello più alto di armonizzazione degli stessi. Le categorie di destinatari dell'intervento della direttiva NIS 2, come brevemente illustrato alla sezione 1, sono state ampliate; infatti, le nuove disposizioni normative sono applicabili anche a soggetti prima non inclusi. Anche il novero dei settori è ampliato ponendo la distinzione tra ª settori ad alta criticità º, di cui all'allegato I, e ª altri settori critici º, di cui all'allegato II. Rientrano nel campo di applicazione della direttiva i soggetti dei settori sopra richiamati che sono considerati almeno medie imprese ai sensi della raccomandazione 2003/361/CE e che prestano i loro servizi o svolgono le loro attività all'interno dell'Unione.
Indipendentemente dalle loro dimensioni, il provvedimento di recepimento si applica anche:

a) ai soggetti che sono identificati come soggetti critici ai sensi della direttiva (UE) 2022/2557;
b) ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico;
c) ai prestatori di servizi fiduciari;
d) ai gestori di registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;
e) ai fornitori di servizi di registrazione dei nomi di dominio;
f) alle pubbliche amministrazioni di cui all'articolo 1, comma 3, legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III del presente decreto legislativo, salvo individuazione di ulteriori categorie di pubbliche amministrazioni in ragione dell'evoluzione del rispettivo grado di esposizione al rischio, della probabilità che si verifichino incidenti e della loro gravità, compreso il loro impatto sociale ed economico;
g) ai soggetti che forniscono servizi di trasporto pubblico locale (allegato IV);
h) agli istituti di istruzione che svolgono attività di ricerca (allegato IV);
i) ai soggetti che svolgono attività di interesse culturale (allegato IV);

j) alle società in house, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175 (allegato IV);
k) ai soggetti dei settori o delle tipologie di cui agli allegati I, II, III e IV, individuati dall' Autorità nazionale competente NIS qualora:
    1) il soggetto sia identificato prima dell' entrata in vigore del presente decreto come operatore di servizi essenziali ai sensi del decreto legislativo 18 maggio 2018, n. 65, di recepimento della direttiva (UE) 2016/1148, ritenuto critico ai sensi del presente decreto;
    2) il soggetto sia l'unico fornitore nazionale di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
    3) una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;
    4) 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;
    5) 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;
    6) 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.

L' attuazione della nuova normativa potrà portare un miglioramento in termini di efficienza nel dominio cibernetico grazie all' instaurazione di misure volte a superare il problema persistente dell' insufficienza del livello di preparazione in materia di cybersicurezza a livello di Stati membri e di società e altre organizzazioni, riducendo altresì i costi supplementari derivanti da incidenti in ambito cibernetico.

Il recepimento della direttiva NIS 2 avrà, dunque, sostanziali ripercussioni in termini di:

- ampliamento ± sostanziale e significativo ± dell' ambito di applicazione a soggetti non considerati dalla precedente direttiva NIS (ovvero P.A. centrale, piccole e microimprese operanti in settori chiave, fornitori di servizi e reti di comunicazione elettronica, indipendentemente dalle loro dimensioni);
- previsione di obblighi per tali soggetti (in particolare quello di notificare non solo gli incidenti ± con una nozione di essi allargata ulteriormente ± ma anche minacce informatiche e quasi incidenti al CSIRT);
- previsione di sanzioni applicabili in proporzione alla gravità delle violazioni.

Il conseguimento del più ampio obiettivo di un livello comune elevato di cybersicurezza nell' Unione postula il rispetto delle misure previste dalla direttiva NIS 2 come recepita dal provvedimento di che trattasi. Esse comportano che i soggetti rientranti nel suo ambito di applicazione debbano adottare ª misure tecniche, operative e organizzative adeguate e proporzionate [¼] alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività 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° (articolo 24 del provvedimento in esame).

Queste misure organizzative includono:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
b) gestione degli incidenti;
c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;
d) sicurezza della catena di approvvigionamento, compresi 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 informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza;
g) pratiche di igiene informatica di base e formazione in materia di cybersicurezza;
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
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, se del caso.

Conseguentemente, per i soggetti cui il provvedimento si rivolge, le richiamate attività potrebbero determinare, nel medio e lungo termine, ulteriori oneri ai quali potranno, tuttavia, corrispondere, nello stesso periodo temporale, a fronte di un maggiore livello di sicurezza, minori costi in termini di ricadute di eventuali incidenti.

L'aumento del livello di preparazione in materia di cybersicurezza, infatti, potrà attenuare la potenziale perdita di entrate a causa di perturbazioni dovute anche allo spionaggio industriale e un approccio volto a prevenire gli incidenti in ambito cibernetico potrà ridurre le ingenti spese che sarebbero invece destinate alla mitigazione di tali incidenti. In tal modo, i vantaggi potranno superare i costi d'investimento.

Per quanto concerne le autorità nazionali competenti e, in particolare per quanto riguarda l'Agenzia per la cybersicurezza nazionale, si evidenzia il significativo impatto sia sulle attività di regolamentazione e attuazione (specie in relazione all'armonizzazione del quadro normativo nazionale, nonché alla definizione delle misure di sicurezza), sia su quelle di vigilanza e coordinamento con i Dicasteri competenti per i settori di riferimento (Autorità di settore). L'impatto sulle attività di monitoraggio, analisi e supporto ai soggetti (Autorità di settore e operatori) e quelle sanzionatorie sarà direttamente proporzionale all'incremento del numero di soggetti vigilati. Tale aumento, unitamente alla rinnovata impostazione con riguardo agli obblighi di notifica determinerà, tra l'altro, un incremento consistente delle segnalazioni di incidente, ivi incluse, potenzialmente, quelle relative a incidenti con impatti transfrontalieri, per le quali è atteso anche un aumento delle attività del Punto di contatto unico. Anche sul fronte della cooperazione a livello europeo è atteso un incremento delle attività ± specie in relazione al primo periodo di applicazione della Direttiva NIS 2 ± con riferimento alle attività in seno al Gruppo di Cooperazione NIS e ai connessi gruppi di lavoro, nonché ± in relazione alla gestione degli incidenti e delle crisi cibernetiche su vasta scala ± all'istituzionalizzazione di EU-CyCLONe, consesso cui la Direttiva, nel formalizzarne il mandato, affida anche ulteriori compiti.

Peraltro, nel medio e lungo termine, l'Autorità nazionale competente e le autorità di settore potranno beneficiare di una maggiore cooperazione tra Stati membri, anche a livello operativo, di un aumento complessivo delle capacità di cybersicurezza a livello nazionale e regionale attraverso l'assistenza reciproca, i meccanismi di revisione tra pari e una migliore panoramica delle imprese chiave e dell'interazione con le stesse.

- principali impatti (benefici e costi attesi) per la collettività

Per i cittadini, il rafforzamento delle politiche di cybersicurezza potrà tradursi prevedibilmente in una riduzione delle perdite di reddito dovute a perturbazioni economiche in quanto un aumento della fiducia globale dei cittadini nell'economia digitale potrà avere un impatto positivo sulla crescita e sugli investimenti. La nuova normativa potrà contribuire ad altri impatti sociali, quali la riduzione dei livelli di criminalità informatica e terrorismo e una maggiore protezione civile, una maggiore sicurezza generale e un funzionamento ininterrotto dei servizi essenziali, sono fondamentali per la società. Inoltre, l'aumento del livello di preparazione di imprese e altre

organizzazioni contro le minacce informatiche può evitare potenziali perdite finanziarie dovute ad attacchi informatici, contribuendo ad evitare ripercussioni sul mercato del lavoro. L'aumento del livello globale di cybersicurezza potrebbe anche prevenire i rischi/danni ambientali in caso di attacco a un servizio essenziale. Questo potrebbe valere in particolare per i settori dell'energia, della distribuzione e dell'approvvigionamento dell'acqua o dei trasporti. Il rafforzamento delle capacità di cybersicurezza potrà portare a un incremento dell'utilizzo delle infrastrutture e dei servizi TIC di ultima generazione, che sono anche più sostenibili dal punto di vista ambientale, e alla sostituzione di infrastrutture preesistenti inefficienti e meno sicure. Ciò contribuirà prevedibilmente anche a ridurre il numero di costosi incidenti informatici, liberando risorse disponibili per investimenti sostenibili.

- distribuzione temporale degli effetti considerati

La distribuzione temporale degli effetti considerati si stima nel medio/lungo termine come sopra ampiamente argomentato.

4.2 Impatti specifici

A. Effetti sulle PMI (Test PMI)
Lo schema di decreto legislativo prevede un'esclusione generale per i micro e piccoli soggetti dal campo di applicazione e un regime di vigilanza *ex post* meno gravoso applicato a un gran numero di nuovi soggetti nell'ambito del campo di applicazione rivisto (i cosiddetti soggetti importanti). Tali misure mirano a ridurre al minimo ed equilibrare gli oneri che gravano sulle imprese e sulle pubbliche amministrazioni. Si sostituisce, inoltre, il complesso sistema di identificazione degli operatori di servizi essenziali con un obbligo generalmente applicabile e si introduce un livello più elevato di armonizzazione degli obblighi di sicurezza e di segnalazione, che mira a ridurre l'onere della conformità, in particolare per i soggetti che forniscono servizi transfrontalieri. La nuova normativa riduce al minimo i costi di conformità per le PMI, in quanto i soggetti sono tenuti ad adottare solo le misure necessarie a garantire un livello di sicurezza dei sistemi informativi e di rete adeguato al rischio presentato.
Altri impatti positivi sono costituiti, altresì, da una semplificazione degli obblighi imposti alle imprese; un elevato livello di armonizzazione che creerà una definizione più efficace degli aspetti operativi; un miglioramento della responsabilizzazione (*accountability*) ed un aumento della condivisione delle responsabilità dei vari portatori di interesse per quanto riguarda le misure di cybersicurezza.

B. Effetti sulla concorrenza
L'intervento normativo non incide negativamente sul corretto funzionamento concorrenziale del mercato e sulla competitività del Paese e non pregiudica l'applicazione delle norme in materia di concorrenza stabilite nel trattato sul funzionamento dell'Unione europea (TFUE).
La nuova disciplina potrà, anzi, favorire e incentivare il funzionamento del mercato interno per i soggetti essenziali e importanti stabilendo norme chiare e generalmente applicabili e armonizzando le norme applicabili nel settore della gestione del rischio di cybersicurezza e della segnalazione di incidenti. Attualmente, infatti, le disparità in questo settore, sia a livello legislativo che di vigilanza, nonché a livello nazionale e dell'Unione, costituiscono ostacoli per il mercato interno perché i soggetti impegnati in attività transfrontaliere fanno fronte a obblighi normativi diversi, con possibili sovrapposizioni, e/o a una loro diversa applicazione a scapito dell'esercizio della loro libertà di stabilimento e la libera prestazione di servizi, e un'applicazione diversificata della normativa di settore ha anche un impatto negativo sulle condizioni della concorrenza nel mercato interno quando si tratta di soggetti dello stesso tipo in Stati membri diversi.

C. Oneri informativi

L'intervento legislativo in esame non introduce, a carico dei cittadini, alcun onere informativo, come definito dall'articolo 14, comma 5-*bis*, della legge 28 novembre 2005, n. 246.

Quanto agli operatori del settore, si richiamano gli oneri informativi connessi all'attività di notifica degli incidenti informatici e alle attività di interlocuzione con le Autorità competenti.

D. Rispetto dei livelli minimi di regolazione europea

Lo schema di decreto legislativo proposto non prevede l'introduzione o il mantenimento di livelli di regolazione superiori a quelli richiesti dalla normativa europea, ai sensi dell'articolo 14, commi 24-*bis*, 24-*ter* e 24-*quater*, della legge 28 novembre 2005, n. 246.

4.3 Motivazione dell'opzione preferita

L'intervento legislativo non presenta svantaggi, ma risulta invece necessario per il recepimento della direttiva NIS 2.

Alla luce delle valutazioni e considerazioni sinora svolte, l'intervento costituisce l'opzione preferita in assenza della quale non sarebbe possibile aggiornare il quadro normativo di riferimento costituito dal decreto legislativo 18 maggio 2018, n. 65, con cui, come accennato, è stata data attuazione alla direttiva NIS.

Senza l'esercizio della delega di cui all'articolo 3 della legge n. 15 del 2024, per la predisposizione del presente decreto legislativo, dunque, non sarebbe, inoltre, possibile recepire correttamente la direttiva NIS 2.

Non si ritiene, pertanto, che opzioni alternative all'intervento legislativo proposto possano essere tenute in considerazione in quanto non di pari o migliore efficacia.

5. MODALITA' DI ATTUAZIONE E MONITORAGGIO

5.1 Attuazione

A seguito dell'analisi di impatto svolta, la valutazione delle condizioni giuridiche, organizzative, finanziarie, economiche, sociali e amministrative che possono incidere in modo significativo sulla concreta attuazione dell'intervento e sulla sua efficacia evidenzia l'incremento della mole di lavoro che esigerà interventi in termini di:

- reclutamento di personale dotato di, o che possa sviluppare, anche una specifica expertise settoriale da impiegare presso l'Agenzia per la cybersicurezza nazionale per gli adempimenti inerenti, in particolare, alle attività di monitoraggio, di vigilanza ed esecuzione;
- acquisizione di strumentazione e mezzi per poter garantire l'efficace assolvimento dei compiti;
- eventualmente, possibili modifiche ordinative.

La responsabilità attuativa dell'intervento normativo ricade, in via prioritaria, sull'Agenzia per la cybersicurezza nazionale.

5.2 Monitoraggio

Il Capo V del provvedimento in esame disciplina, all'articolo 34, gli aspetti generali relativi al monitoraggio, alla vigilanza e all'esecuzione, che si concretizzano in attività di analisi e supporto; di verifica ed ispezioni; di adozione di misure di esecuzione e di irrogazione delle sanzioni,

attribuendo all'Autorità nazionale competente NIS la vigilanza sull'adempimento degli obblighi previsti dalla nuova Direttiva e sui relativi effetti in materia di sicurezza della rete e dei sistemi informativi da parte degli operatori di servizi essenziali e importanti.

In particolare, l'articolo 35 dello schema prevede che l'Autorità nazionale competente NIS garantisca un'attività di monitoraggio, analisi e supporto ai soggetti sulla base delle informazioni trasmesse tramite registrazione sulla piattaforma digitale, resa disponibile dall'Agenzia per la cybersicurezza nazionale, nonché delle eventuali rendicontazioni o dell'aggiornamento dei dati inseriti in piattaforma al momento della registrazione.

Tale monitoraggio è funzionale all'aggiornamento periodico dell'elenco dei soggetti essenziali e importanti da trasmettere alla Commissione europea almeno ogni due anni, come prescritto dall'articolo 3, paragrafo 3, della Direttiva.

A livello europeo, ai sensi dell'articolo 40 della direttiva NIS 2, entro il 17 ottobre 2027 e successivamente ogni 36 mesi, la Commissione riesamina il funzionamento della direttiva NIS 2 e presenta una relazione in proposito al Parlamento europeo e al Consiglio, che tiene conto delle relazioni del gruppo di cooperazione e della rete di CSIRT sull'esperienza acquisita a livello strategico e operativo.

A livello nazionale, l'articolo 35 del decreto legislativo prevede un'attività di monitoraggio che coinvolge l'Autorità competente NIS, le Autorità di settore e i soggetti pubblici e privati a cui si applica il decreto legislativo.

CONSULTAZIONI SVOLTE NEL CORSO DELL'AIR

1. Descrizione delle consultazioni svolte e delle relative modalità di realizzazione

Nelle more dell'adeguamento alla NIS 2, tenuto conto del significativo impatto che la rinnovata disciplina avrà sul tessuto economico nazionale, sono state poste in essere diverse iniziative per sensibilizzare i soggetti che operano nei settori cui si applicherà la nuova Direttiva ed è stato avviato un dialogo con gli stessi soggetti volto a individuare ulteriori elementi da valutare nelle successive fasi dell'attività legislativa e regolamentare di attuazione.

A tale riguardo, diversi eventi sono stati organizzati anche da organismi europei come ENISA, dal tessuto imprenditoriale e da enti attivi nel partenariato pubblico-privato.

Nel periodo di riferimento, sono state altresì avviate specifiche iniziative a supporto dei soggetti inseriti nel PSNC per sensibilizzarli sull'imminente recepimento della Direttiva NIS2. A partire da aprile 2023 è stato, infatti, condotto un ciclo di oltre 30 riunioni settoriali in cui sono stati invitati gruppi omogenei di soggetti inseriti nel Perimetro, alla presenza delle rispettive amministrazioni settorialmente competenti.

Al contempo, sono stati consolidati i rapporti con le 5 amministrazioni centrali, autorità di settore NIS (Ministero dell'economia e finanze-MEF, Ministero delle imprese e del made in Italy-MIMIT, Ministero dell'ambiente e della sicurezza energetica, Ministero delle infrastrutture e trasporti e Ministero della salute), attraverso periodiche riunioni, al fine di monitorare lo stato di attuazione della prima Direttiva NIS e avviare le discussioni relative agli aspetti pratici di recepimento della Direttiva NIS 2. In quel contesto è anche stata confermata la rilevanza del ruolo delle Regioni e delle Province autonome, in relazione ad alcuni settori che rientrano nell'ambito di applicazione della nuova Direttiva, ed è stata conseguentemente avviata una interlocuzione con la Conferenza delle Regioni e delle Province autonome in vista di un suo prossimo coinvolgimento per le fasi attuative di rispettiva competenza.

Al fine di una adeguata predisposizione del presente decreto legislativo e del conseguente corretto recepimento della direttiva NIS 2, sono stati sentiti e coinvolti, a partire da settembre 2023, i rappresentanti delle Autorità di settore NIS, per individuare le criticità emerse in fase di implementazione della prima normativa e superarle in sede di recepimento della NIS2.

In particolare, sono stati organizzati molteplici incontri, a livello tecnico, con il Ministero delle imprese e del made in Italy (MIMIT), con il Ministero delle infrastrutture e dei trasporti (MIT), con il Ministero dell'economia e delle finanze (MEF), con il Ministero della salute e con il Ministero dell'ambiente e della sicurezza energetica (MASE) per pianificare attività congiunte di *awareness*, attraverso appositi tavoli di settore, nei confronti dei soggetti già vigilati, in continuità con il lavoro svolto in sede di identificazione, monitoraggio e aggiornamento degli OSE ai sensi della precedente Direttiva, e al contempo per verificare l'eventuale competenza delle stesse amministrazioni su nuovi settori, sotto-settori e tipologie di soggetti NIS2.

Per i sotto-settori e per le tipologie dei soggetti che fanno capo al settore "Fabbricazione", è stata avviata una interlocuzione con Confindustria al fine di individuare eventuali enti/organismi o dipartimenti di riferimento in relazione a ciascuna specifica area produttiva.

2. Elenco dei soggetti che hanno partecipato a ciascuna delle consultazioni

I soggetti consultati in fase di redazione del decreto legislativo in esame hanno partecipato ad appositi tavoli di settore convocati da ciascun Ministero in qualità di autorità dei settori già NIS.

In particolare, nel corso delle riunioni con le Autorità di settore NIS, periodicamente riunite coinvolgendo via via le Amministrazioni che hanno riconosciuto una propria competenza su settori di nuova introduzione nella implementanda Direttiva, si è proceduto ad una programmazione di tavoli di settore dedicati, convocati da ciascun Ministero per i settori di propria competenza.

Pertanto, dal mese di gennaio sono stati convocati dalle rispettive Autorità di settore, con la partecipazione di ACN, i tavoli dei settori "Infrastrutture e Fornitori di servizi digitali" e "TELCO" (presso il MIMIT), i tavoli con rappresentanti del settore "Trasporti" (presso il MIT), i tavoli dei settori "Energia" e "Acqua potabile" (presso il MASE) e il tavolo del settore "Sanitario" presso il Ministero della salute.

A questi ultimi hanno preso parte associazioni di categoria e soggetti privati su invito delle Autorità di settore competenti, con un'adesione significativa soprattutto con riferimento ai dell'Energia e dell'Acqua potabile.

A seguito delle citate interlocuzioni con Confindustria, quest'ultima ha organizzato un evento dedicato ai suoi consociati (circa 600 aderenti anche in modalità VTC) di tutti i settori impattati dalla nuova disciplina per consentire una più capillare informazione circa l'imminente recepimento della Direttiva NIS2.

In considerazione della capillare attività informativa avviata nei confronti di un elevato numero di soggetti, alcuni dei quali già sottoposti a vigilanza in conformità con il quadro nazionale di cybersicurezza, non è possibile fornire un elenco dei soggetti che hanno partecipato alle citate consultazioni.

3. Periodi in cui si sono svolte le consultazioni.

Le interlocuzioni volte a sensibilizzare i soggetti che operano nei settori cui si applicherà la nuova Direttiva sono state avviate già dal mese di aprile 2023.

A partire dal 21 settembre 2023, il tavolo con le Autorità di settore NIS1 si è poi riunito con cadenza pressoché mensile, coinvolgendo via via le Amministrazioni che hanno riconosciuto una

propria competenza su settori di nuova introduzione. Nell'ottavo e ultimo incontro, svoltosi il 31 maggio u.s., sono intervenute tutte le Autorità di settore individuate anche alla luce della proposta di schema elaborata da ACN.

Inoltre, dal mese di gennaio u.s. hanno avuto luogo i primi 6 tavoli di settore come sopra descritti e, con riferimento in particolare al settore "Trasporti", in due giornate sono stati separatamente incontrati i soggetti dei sotto-settori "Trasporto aereo", "Trasporto ferroviario", "Trasporto per le vie d'acqua" e "Trasporto su strada".

4. Principali risultati emersi dalle consultazioni.

A seguito dei citati incontri, alcune Autorità di settore hanno avviato delle interlocuzioni al proprio interno e con organismi aggregatori o di vigilanza del settore di competenza per una più agevole individuazione dell'ambito di applicazione della NIS2, i cui esiti sono stati presi in considerazione in fase di redazione dello schema di Decreto legislativo di recepimento della Direttiva NIS2.

In particolare:

· il Ministero della salute ha coinvolto AIFA per l'individuazione dei soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici e dei soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica;

· il Ministero dell'Ambiente e della Sicurezza Energetica (MASE) ha avviato una interlocuzione con ARERA per i servizi idrici (acqua potabile e acque reflue) e la gestione dei rifiuti urbani ed assimilati;

· il Ministero dell'Università e della ricerca (MUR), al fine di definire i criteri per l'individuazione dei soggetti vigilati ai sensi della nuova Direttiva, ha previsto il coinvolgimento della Conferenza dei rettori delle Università italiane (CRUI), e quello degli enti di ricerca con l'eventuale coinvolgimento della Consulta dei presidenti degli enti di ricerca (ConPER) o della Conferenza permanente dei Direttori Generali degli Enti Pubblici di Ricerca Italiani (CODIGER) e l'inquadramento da adottare per altre realtà sensibili come il CNR.

Anche sulla base delle criticità emerse nel corso dei primi tavoli di settore con i soggetti già NIS, in merito all'individuazione dell'ambito di applicazione della nuova Direttiva, è stata evidenziata l'importanza del criterio dimensionale ± introdotto dalla lettera a) del primo comma dell'articolo 3 della Direttiva ± pertanto recepita nell'articolato all'articolo 3 relativo all'ambito di applicazione. Al contempo, è emersa l'esigenza di disciplinare al meglio i parametri giurisdizionali per le imprese che pur non avendo sede legale in Italia, forniscono sul territorio nazionale prodotti e servizi (oltre all'esempio tipico dei *registrar* si è fatto riferimento a dispositivi medici e prodotti farmaceutici, oppure ad autoveicoli prodotti all'estero ma immessi come semilavorati nelle filiere produttive italiane). È stato pertanto introdotto l'articolo 5 su Giurisdizione e territorialità che declina in modo più dettagliato quanto prescritto dalla Direttiva.

È stata sottolineata anche la necessità di definire al meglio i criteri di applicazione della Direttiva NIS2 ai Gruppi di imprese e alle catene di approvvigionamento, per una implementazione proporzionata e graduale degli obblighi in capo ai soggetti altamente critici e critici di tutti i settori NIS2, nel rispetto della lettera della Direttiva. Sul punto il criterio già previsto dalla Direttiva è stato recepito dall'articolo 31 del testo in esame sulla proporzionalità e gradualità degli obblighi, che verrà meglio declinato con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS.

Ulteriori risultati delle consultazioni hanno riguardato:

· la necessità di regolamentare nel dettaglio l'attività dei tavoli di settore con linee guida e un nuovo *framework* nazionale e sulla possibilità, da parte di ciascuna Autorità di settore, di favorire la registrazione dei soggetti essenziali e importanti attraverso il caricamento su piattaforma dei soggetti già individuati come OSE ai sensi della Direttiva NIS;

· l'opportunità di prevedere termini di implementazione degli obblighi che risultino compatibili con i cicli di *budge*t da allocare;

· l'esigenza di procedere all'individuazione degli enti di ricerca quali soggetti essenziali o importanti, tenendo in giusta considerazione i diversi livelli di criticità dei singoli soggetti;

· i criteri di individuazione dei soggetti che svolgono attività di interesse culturale.

Infine, in attuazione dei sopracitati criteri di proporzionalità e gradualità in fase di implementazione della Direttiva, è stata proposta una *roadmap* della fase regolamentare discendente dal decreto legislativo in oggetto, poi declinata nell'articolo 40 dello stesso articolato.

PERCORSO DI VALUTAZIONE

L'AIR è stata effettuata dalla Presidenza del Consiglio dei ministri sulla base degli elementi informativi al momento disponibili.