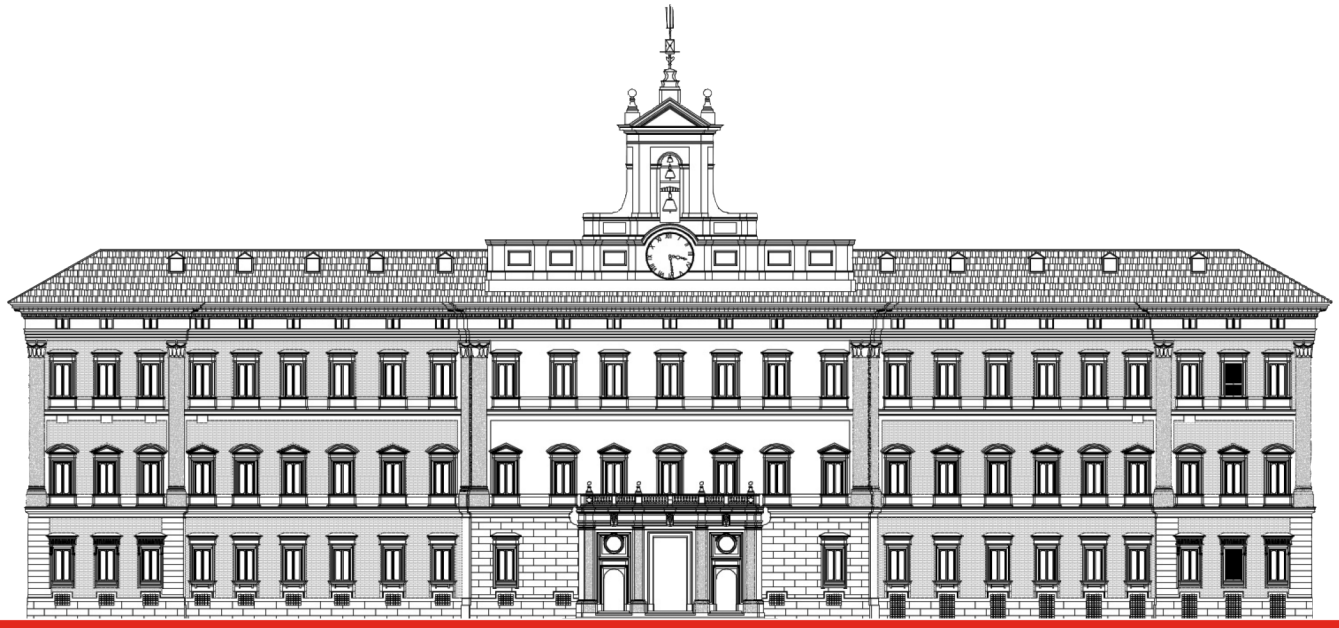
Camera dei deputati

XIX LEGISLATURA



Documentazione per le Commissioni

ESAME DI ATTI E DOCUMENTI DELL'UNIONE EUROPEA

Elementi per la verifica di sussidiarietà

Il pacchetto cibersicurezza

(Proposta di regolamento COM(2026)11)

(Proposta di direttiva COM(2026)13)

n. 149

31 marzo 2026

Camera dei deputati

XIX LEGISLATURA

Documentazione per le Commissioni

ESAME DI ATTI E DOCUMENTI DELL'UNIONE EUROPEA

Elementi per la verifica di sussidiarietà

Il pacchetto cibersicurezza

(Proposta di regolamento COM(2026)11)

(Proposta di direttiva COM(2026)13)

n. 149

31 marzo 2026

Il dossier è stato curato dal **SERVIZIO PER I RAPPORTI CON L'UNIONE EUROPEA** (☏ 066760.2145 - ✉ *rue_segreteria@camera.it* - 𝕏@CD_europa - europa.camera.it).

I N D I C E

DATI IDENTIFICATIVI

Tipo di atto	*Proposta di regolamento COM(2026)11* *Proposta di direttiva COM(2026)13*
Data di adozione	*20 gennaio 2026*
Base giuridica	*Articolo 114 TFUE*
Settori di intervento	*Industria dell'informatica; criminalità informatica; sicurezza d'approvvigionamento; certificazione comunitaria; funzionamento istituzionale; Agenzia dell'Unione europea per la cibersicurezza; sicurezza delle informazioni; guerra dell'informazione; catena di approvvigionamento; formalità amministrativa; gestione del rischio; sicurezza delle infrastrutture critiche*
Esame presso le istituzioni dell'UE	*Procedura legislativa ordinaria*
Assegnazione	*24 marzo 2026 - Commissioni riunite: I Commissione "Affari costituzionali" e IX Commissione "Trasporti"*
Termine per il controllo di sussidiarietà	*13 maggio 2026*
Segnalazione da parte del Governo	*Sì*
Relazione del Governo ex. art. 6 della legge 234	*No*

IL PACCHETTO CIBERSICUREZZA

Il pacchetto legislativo in materia di cibersicurezza è parte del più ampio **processo di rafforzamento della resilienza digitale dell'Unione europea**, in un contesto internazionale caratterizzato da una crescente interconnessione tra sicurezza informatica, stabilità economica e competizione geopolitica.

Le iniziative in esame segnano **un'evoluzione significativa dell'approccio europeo alla cibersicurezza**, che da ambito prevalentemente tecnico-regolatorio tende progressivamente a configurarsi come **leva strategica per la tutela delle infrastrutture critiche**, la **protezione delle catene di approvvigionamento** ed il **rafforzamento dell'autonomia tecnologica dell'Unione**.

In tale prospettiva, il pacchetto persegue una duplice finalità:

- da un lato, **semplificare e rendere più efficace il quadro normativo vigente**, in particolare attraverso la revisione del mandato dell'ENISA e dei meccanismi di certificazione;
- dall'altro, introdurre **strumenti più incisivi per la gestione dei rischi sistemici**, inclusi quelli di natura non tecnica connessi alle dipendenze strategiche da Paesi terzi.

Finalità e oggetto

Il **pacchetto** è stato presentato dalla Commissione europea il 20 gennaio 2026 ed è composto da:

- una proposta di regolamento (*c.d.* proposta di regolamento sulla cibersicurezza 2) relativa all'**Agenzia dell'UE per la cibersicurezza** (ENISA), al **quadro europeo di certificazione della cibersicurezza** (ECCF) e alla sicurezza delle catene di approvvigionamento delle TIC (tecnologie dell'informazione e della comunicazione) che abroga il regolamento sulla cibersicurezza (*c.d.* ***Cybersecurity Act***);
- una proposta di direttiva che modifica la direttiva sulle misure per un livello comune elevato di cibersicurezza nell'Unione (*c.d.* **direttiva NIS 2**) per quanto riguarda le misure di semplificazione e l'allineamento alla proposta di regolamento sulla cibersicurezza 2.

Rinviando per maggiori dettagli sulle specifiche misure al paragrafo del presente dossier dedicato ai principali contenuti delle proposte, il futuro regolamento sulla cibersicurezza (***Cybersecurity Act* 2**) si articola, secondo la Commissione europea, attorno a **tre assi portanti**:

1) il **rafforzamento** dell'efficacia e la **semplificazione** della **certificazione** europea di cibersicurezza per garantirne una maggiore fruibilità, prevedibilità e una migliore integrazione nel mercato;

2) la **definizione** più netta della **relazione** tra i processi di **certificazione** e i **rischi di natura non tecnica**, con particolare riferimento alla sicurezza delle catene di approvvigionamento;
3) la **riorganizzazione** del mandato dell'**ENISA** mirata a incrementarne le funzioni di supporto operativo e di fornitura di servizi, eliminando ogni possibile incertezza interpretativa sulle sue mansioni.

L'aggiornamento del regolamento sulla cibersicurezza permetterà anzitutto, secondo la Commissione, di sottoporre i beni e i servizi rivolti ai consumatori dell'UE a **test di sicurezza più efficaci**, avvalendosi di un rinnovato **ECCF**. Tali schemi certificativi, gestiti dall'ENISA, offriranno alle imprese lo strumento per attestare la conformità alla legislazione dell'UE, riducendo al contempo gli oneri amministrativi e i costi, traducendosi così in un vantaggio competitivo per le imprese dell'UE.

Il nuovo regolamento introduce inoltre soluzioni finalizzate a rendere più agevole il rispetto degli **standard di sicurezza informatica** e dei **doveri di gestione dei rischi** per le imprese che operano nell'UE. Le modifiche proposte puntano a semplificare le norme giurisdizionali, a ottimizzare le procedure di raccolta dati relativi agli attacchi *ransomware* e a facilitare la **vigilanza** sui soggetti che operano su scala transfrontaliera, grazie a una funzione di coordinamento più incisiva affidata all'ENISA.

Il *ransomware* è un programma informatico dannoso che può "infettare" un dispositivo digitale bloccando l'accesso a tutti o ad alcuni dei suoi contenuti, per poi chiedere un riscatto (in inglese, "*ransom*") da pagare per "liberarli".

Quanto all'**ENISA,** con la nuova disciplina, essa fornirà un ausilio ancora più strutturato alle imprese e ai portatori di interessi attivi nell'UE, diffondendo **allerte tempestive** riguardanti minacce e incidenti informatici. Agendo in sinergia con Europol e con gruppi di intervento per la sicurezza informatica (CSIRT) in caso di incidente, l'Agenzia sosterrà le imprese sia in fase di risposta agli attacchi *ransomware*, sia nelle successive fasi di ripristino delle attività. Spetterà inoltre all'ENISA la gestione operativa dello **sportello unico dedicato alla segnalazione degli incidenti**, così come delineato nel pacchetto dell'*omnibus* digitale.

La Commissione europea ha presentato la proposta di regolamento che **semplifica** il **quadro legislativo** del settore **digitale**, contenente l'introduzione dello sportello unico, nell'ambito del settimo pacchetto di semplificazione, *c.d.* **omnibus digitale** (v. dossier RUE). Presso la Camera, in esito all'esame ai fini della verifica della conformità al principio di sussidiarietà, la **Commissione Politiche dell'UE** ha adottato, il 24 febbraio 2026, un documento recante una **valutazione conforme** sull'intero pacchetto. Ai sensi dell'articolo 127, comma 1, del Regolamento della Camera, la **Commissione Trasporti** ha **avviato** il 4 marzo 2026 l'**esame di merito** sulla proposta di regolamento che semplifica il quadro legislativo del settore digitale.

La **proposta di direttiva**, invece, ha l'**obiettivo generale** di **semplificare** il rispetto degli **obblighi di cibersicurezza** in modo da garantire un'attuazione razionalizzata e coerente del quadro giuridico in materia di cibersicurezza, semplificando la conformità alle norme. A tal fine, rinviando per maggiori dettagli al paragrafo dedicato, la Commissione propone misure volte a:

1) **consentire** ai **soggetti** regolamentati di **ottenere certificati** nell'ambito dei sistemi organizzativi di certificazione della cibersicurezza **sviluppati nell'ambito** dell'**ECCF**;
2) **attribuire** all'**ENISA** un **ruolo di sostegno** agli Stati membri nella vigilanza di tali soggetti.

Il dibattito in seno al Consiglio

Da fonti informali si apprende che in sede di Consiglio tutti gli Stati membri avrebbero anticipato una **riserva di esame** essendo ancora impegnati ad approfondire le misure prospettate dalle proposte. Complessivamente le prime reazioni dei governi si sarebbero concentrate su quattro filoni principali:

1) la necessità di **dare continuità** al **lavoro** sulla **certificazione**, evitando che il negoziato sulla proposta di revisione del *Cybersecurity Act* si traduca in una sospensione di fatto degli schemi in corso, per esempio in ambito *cloud*;
2) prevedere **risorse finanziarie adeguate** e certe a favore di tutti gli aspetti della cibersicurezza;
3) **valutare** gli **impatti** delle modifiche prospettate alla direttiva NIS 2 **relative** all'**implementazione nazionale**;
4) garantire la **complessiva coerenza** del *Cybersecurity Act 2* con le altre politiche UE sotto il profilo della sicurezza, della semplificazione e della politica industriale.

La posizione del Governo italiano

Secondo fonti informali, il **Governo italiano** ha accolto favorevolmente il pacchetto di misure, in particolare con riferimento alla protezione delle catene di approvvigionamento dove un approccio puramente reattivo risulterebbe strutturalmente insufficiente. L'Italia avrebbe inoltre sottolineato la coerenza dell'impianto del pacchetto utile ad evitare vuoti normativi ed evidenziato l'esigenza di adottare un **approccio** "***simplicity by design***" e auspicando, con la convergenza della Francia, che il rafforzamento dell'ENISA non comporti una dispersione delle funzioni o sovrapposizioni operative rispetto agli Stati membri e ai CSIRT.

Sempre da fonti informali si apprende la presentazione negli scorsi mesi di un **documento informale**, firmato dall'Italia e da altri Stati membri, riguardante il mandato dell'ENISA nel contesto della revisione del regolamento sulla cibersicurezza.

Il documento delinea una visione strategica per l'**ENISA**, sottolineando la necessità di rafforzarne il ruolo come fulcro di conoscenza e coordinamento tecnico senza però trasformarsi in un CSIRT di livello europeo. In particolare;

a) l'ENISA dovrebbe consolidarsi come il principale **centro di competenze** dell'UE, supportando gli Stati membri nell'attuazione delle normative sulla cibersicurezza. Ciò in soprattutto nella **capacità di previsione**: l'Agenzia dovrebbe anticipare i rischi legati alle tecnologie emergenti, con un *focus* particolare sull'**intelligenza artificiale** e il **calcolo quantistico**, fornendo agli Stati membri gli strumenti conoscitivi per affrontare queste sfide;
b) l'Agenzia dovrebbe mantenere una funzione **orizzontale e intersettoriale**, collaborando strettamente con le altre agenzie UE (come Europol, Agenzia europea per la difesa - EDA e il Centro europeo di competenza per la cibersicurezza - ECCC). In particolare, essa dovrebbe essere consultata sistematicamente prima e dopo la presentazione di nuove norme, politiche o programmi di lavoro. Il suo compito principale dovrebbe rimanere quello di facilitare la cooperazione tra le reti nazionali (CSIRT Network e EU-CyCLONe), migliorando la consapevolezza comune sulla situazione delle minacce (*situational awareness*) attraverso una gestione dei dati trasparente e condivisa, tenendo conto in particolare del Programma dell'UE per la cibersicurezza (*EU cyber blueprint*);
c) l'ENISA dovrebbe diventare un **laboratorio per strumenti, tecniche e infrastrutture di cibersicurezza** a supporto dei CSIRT degli Stati membri, attraverso il coinvolgimento di esperti nazionali, riducendo le dipendenze strategiche da servizi esterni di cibersicurezza e rafforzando la partecipazione europea a programmi come il CVE rivolto a identificare vulnerabilità ed esposizioni comuni in materia di sicurezza informatica, in linea con le raccomandazioni della Rete dei CSIRT. Gli sforzi dovrebbero concentrarsi sul mantenimento del programma CVE come standard riconosciuto a livello globale, in modo da rafforzare le capacità dell'Europa in questo ambito critico;
d) per garantire un mercato unico digitale sicuro, l'ENISA dovrebbe aumentare la propria collaborazione negli organismi di **standardizzazione europei**, assicurando che le norme tecniche – esistenti ed emergenti – siano in linea con le politiche, le norme e i regolamenti europei. Per quanto riguarda il Quadro europeo di **certificazione della cibersicurezza**, il processo deve essere semplificato e reso più trasparente, definendo con chiarezza i confini tra le responsabilità della Commissione europea e quelle dell'Agenzia;
e) andrebbe assicurata l'autonomia e la sostenibilità finanziaria dell'Agenzia. In particolare, il Consiglio di amministrazione dovrebbe avere un ruolo più forte nel definire le priorità. Non dovrebbero essere assegnati nuovi compiti all'ENISA senza il preventivo accordo del Consiglio di amministrazione. Per mantenere competenze di alto livello e gestire infrastrutture critiche

internamente, l'Agenzia necessiterebbe anche di **finanziamenti adeguati e a lungo termine**. Solo con una stabilità finanziaria, secondo gli Stati membri firmatari, l'ENISA potrà investire in progetti strategici, conservare il patrimonio di conoscenze istituzionali e sviluppare competenze a lungo termine, tutti elementi necessari per proteggere l'architettura digitale dell'Unione.

Le posizioni degli altri Stati membri

La **Francia** avrebbe sostenuto la necessità di limitare le disposizioni relative alla certificazione ai rischi tecnici di cibersicurezza poiché i profili non tecnici, tra cui quelli riguardanti la sovranità dei dati, le dipendenze strategiche e i fattori geopolitici, dovrebbero essere trattati nell'ambito dei lavori sulla sicurezza delle catene di approvvigionamento nel quadro più ampio della strategia di sicurezza economica e tecnologica dell'UE.

Ungheria e **Slovenia** avrebbero invece evidenziato come la proposta di revisione del *Cybersecurity Act* interferisca in ambiti sensibili della sicurezza nazionale, ricordando il solo parziale successo di precedenti regolazioni europee in questi ambiti, come, a titolo esemplificativo, il 5G. I due Paesi, assieme alla **Croazia**, avrebbero anche sottolineato l'esigenza che ogni analisi delle dipendenze nell'ambito delle catene di produzione TIC tenga pienamente conto delle potenziali ricadute economiche e della disponibilità di tecnologie alternative.

Contesto, motivazioni dell'intervento, consultazione dei portatori di interessi e valutazione di impatto

La relazione sulla valutazione dell'ENISA e del quadro europeo di certificazione della cibersicurezza

Contestualmente alla presentazione delle proposte legislative in esame la Commissione europea ha pubblicato la **relazione** sulla **valutazione** dell'**ENISA** e del **quadro europeo** di **certificazione della cibersicurezza** (ECCF) ai sensi dell'articolo 67 del regolamento sulla cibersicurezza.

La relazione ha individuato diverse **sfide** cui l'**ENISA** deve far fronte, tra cui la **carenza di personale** sufficiente che ha influenzato negativamente la reattività dell'Agenzia a far fronte alla rapida evoluzione delle minacce informatiche. Inoltre, sottolinea lo **scarso coordinamento** con altri enti, come il Centro europeo di competenza per la cibersicurezza, l'Agenzia europea per la sicurezza marittima (EMSA) e il *Joint Research Center* della Commissione europea, che potrebbe generare sovrapposizioni e inefficienze nell'ecosistema europeo della cibersicurezza. Allo stesso modo, infine, sostiene sia necessaria una **relazione più stretta** con gli **Stati membri** per rafforzare la condivisione delle informazioni.

Per quanto riguarda l'**ECCF**, invece, la relazione evidenzia **alcune debolezze** significative, tra cui in particolare la **lunghezza dei processi di adozione** dei sistemi e la **complessità tecnica** che ne impediscono un'efficace attuazione.

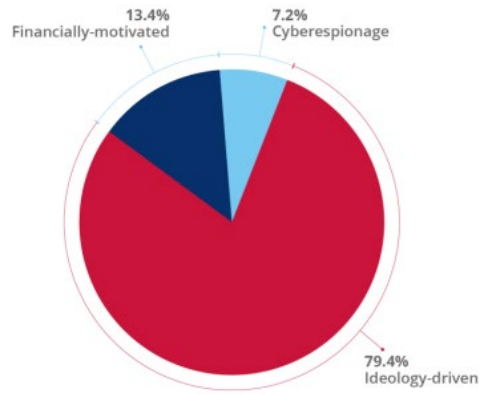
Per esempio, afferma la Commissione europea, per il primo sistema europeo di certificazione della cibersicurezza basato su criteri comuni **sono passati,** dall'avvio alla sua effettiva adozione, **57 mesi**.

Tali ritardi, dovuti anche dagli squilibri presenti in termini di risorse e competenze disponibili all'interno dell'UE, incidono sull'efficacia complessiva del quadro. Per questi motivi, la valutazione sostiene la necessità di una **revisione** delle strutture di ***governance*** e lo sviluppo di **processi decisionali semplificati**.

I rischi di cibersicurezza nell'UE

La **relazione** **sulla panoramica delle minacce 2025** pubblicata da ENISA nell'ottobre scorso evidenzia come circa l'**80%** degli incidenti registrati nell'UE tra il luglio 2024 e il giugno 2025 siano riconducibili ad **attività** di **matrice ideologica** condotta da *hacker*.

Fig. 6 - Distribution of assessed objectives.
Source: ENISA dataset



La relazione sostiene che la maggior parte di tali attacchi consiste in azioni informatiche che mirano a sovraccaricare un sito o in *server* fino a renderlo inaccessibile agli utenti legittimi (*c.d.* **azioni DoS**, *Denial of Service*).

ENISA sostiene che i picchi di attività di queste azioni DoS **coincidono** sistematicamente con **eventi geopolitici rilevanti** (come dichiarazioni di sostegno all'Ucraina o elezioni nazionali) per cui, nonostante l'impatto operativo reale sia spesso marginale, si può ritenere che tali operazioni si inseriscano in campagne di manipolazione dell'informazione più ampie.

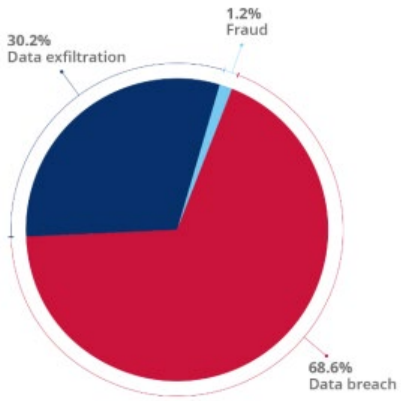
Circa il **13,5%** degli incidenti sono invece riconducibili alla **criminalità informatica**, che costituisce tuttavia, secondo la relazione, la minaccia più impattante in termini concreti. L'**Italia** rappresenta il **secondo Paese** dell'Unione

più colpito, dopo la Germania, in termini di richieste di risarcimento in relazione a *ransomware* e violazioni dei dati. Infine circa il **7%** degli incidenti è riconducibile ad **attività** di **Stati terzi**.

Tra le intrusioni registrate dall'ENISA, il 68,6% ha determinato fughe di dati messi in vendita su siti di criminali informatici. In particolare, il 2,8% di queste fughe è stato presentato come conseguenza diretta di un attacco *ransomware*. L'esfiltrazione di dati, compreso il furto di credenziali (8,9%) e la raccolta strategica di dati (21,3%), ha rappresentato il 30,2% degli incidenti.

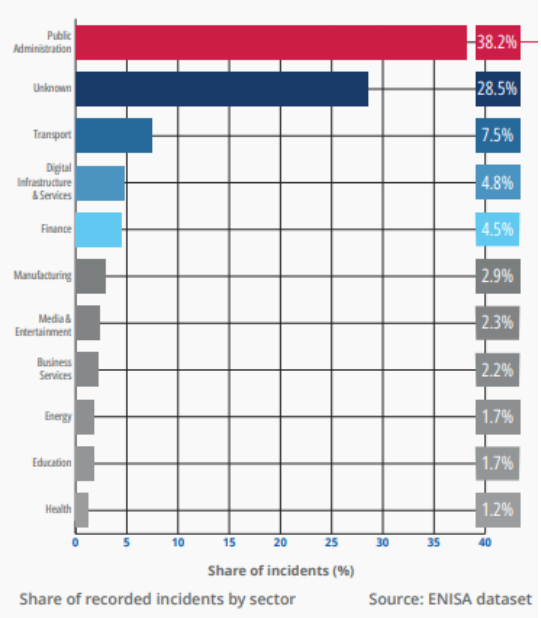
Secondo gli ultimi dati Eurostat, nel 2023 il **21,5%** delle **imprese** dell'UE ha subito **incidenti di sicurezza informatica** con conseguenze di vario tipo, come l'indisponibilità dei servizi informatici, la distruzione o il danneggiamento dei dati o la divulgazione di dati riservati.

Fig. 4 - Outcome of identified intrusions.
Source: ENISA dataset



I primi cinque settori oggetto di attacchi informatici risultano essere la pubblica amministrazione (38,2%), i trasporti (7,5%), le infrastrutture e i servizi digitali (4,8%), il settore finanziario (4,5%) e l'industria manifatturiera (2,9%).

La relazione sottolinea la stretta corrispondenza tra tali settori e quelli esplicitamente definiti dalla direttiva NIS 2 come essenziali e quindi soggetti ad obblighi più stringenti in materia di cibersicurezza. In particolare, evidenzia ENISA, il 53,7% del numero totale di incidenti registrati è avvenuto in settori considerati essenziali ai sensi della direttiva.

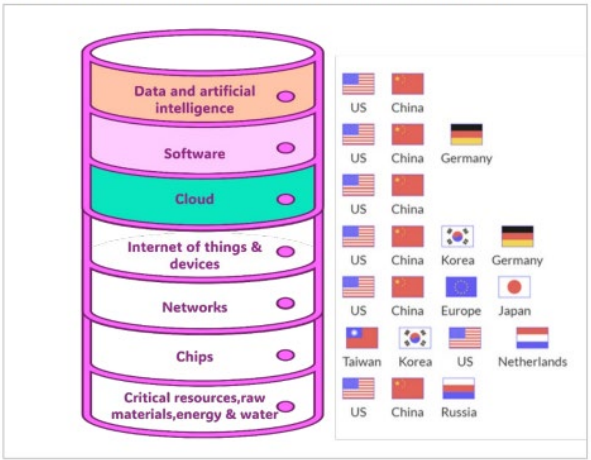


Un **elemento trasversale** che caratterizza tutte e tre le categorie di attacchi informatici è il **ruolo crescente** dell'**IA**. Infatti, osserva la relazione, l'implementazione su larga scala e la disponibilità di tali sistemi generano un nuovo livello di scalabilità nelle attività dannose da parte degli aggressori.

I rischi legati alle dipendenze strategiche verso Paesi terzi

Uno studio commissionato dalla Commissione per l'industria, la ricerca e l'energia (ITRE) del Parlamento europeo pubblicato nel dicembre 2025 ha analizzato la **sistemica dipendenza** dell'UE da fornitori di *software* e servizi *cloud* extra-UE. Come emerge dalla figura che segue, gli **USA** e la **Cina controllano** sostanzialmente tutti i **livelli critici** delle **tecnologie IT**.

Figure 2: Key countries controlling the layers of the digital stack



Source: EuroStack.

In questo contesto l'UE è soggetta a una **dipendenza** non solo economica ma anche **strategica**. Lo studio evidenzia alcuni rischi principali di tale dipendenza, quali l'esposizione a interruzioni improvvise di accesso a servizi *cloud* essenziali in seguito a decisioni politiche estere e la possibile esposizione di dati dei cittadini e delle istituzioni europee presenti su infrastrutture digitali di fornitori esteri. Dall'analisi emergono inoltre **vulnerabilità** delle **catene di approvvigionamento**, considerato, per esempio, che l'Unione importa circa il 90% dei semiconduttori avanzati e che i fornitori di servizi *cloud* statunitensi detengono circa il 69% del mercato europeo, contro il 13% detenuto dai fornitori europei.

Il rapporto Draghi sostiene che, data la posizione dominante dei fornitori USA, l'UE deve trovare un **compromesso** tra la **garanzia di accesso** alle tecnologie di cui ha bisogno e la **promozione** dell'**industria *cloud* domestica**. Considerata infatti la mole di investimenti che sarebbero necessari per colmare il *gap* esistente, Draghi non considera opportuno cercare di sviluppare imprese in grado di confrontarsi con i fornitori di *cloud* statunitensi per non disperdere risorse da settori con migliori prospettive innovative per l'UE. Tuttavia, ritiene fondamentale lo sviluppo di un'industria domestica competitiva in grado di soddisfare la domanda di soluzioni sovrane.

Per approfondimenti sul rapporto Draghi si veda il dossier predisposto dal Servizio RUE della Camera dei deputati.

I tentativi dell'UE di ridurre progressivamente l'esposizione alle dipendenze strategiche brevemente descritte, si devono tradurre, sostiene lo studio, non solo nella **mappatura sistemica** delle **dipendenze critiche** e in una **diversificazione** dei **fornitori** nelle infrastrutture sensibili, ma anche nel **rafforzamento** della capacità di **rilevamento** delle **minacce di cibersicurezza**.

I profili evidenziati confermano come la cibersicurezza si configuri sempre più come **una componente essenziale della sicurezza economica e tecnologica dell'Unione**, ponendo in evidenza la necessità di strumenti normativi in grado di affrontare non solo i rischi tecnici, ma anche quelli **derivanti da fattori geopolitici e da dipendenze strategiche**.

Le motivazioni dell'intervento

La Commissione ha presentato il pacchetto di misure in materia di cibersicurezza come **risposta** alle **esigenze** manifestate dagli **Stati membri** e dai **portatori di interesse**, inserendolo in uno scenario caratterizzato da un **progressivo peggioramento delle minacce** e da una sollecitazione sistemica sempre più marcata nei confronti dell'ecosistema digitale dell'Unione, dove gli attacchi informatici crescono sia in termini di volume che di complessità.

Tenendo conto delle numerose norme di settore emanate successivamente all'approvazione del regolamento sulla cibersicurezza del 2019, e considerando quanto velocemente stia mutando lo scenario delle minacce informatiche, la Commissione ha ritenuto necessario rivedere il mandato dell'ENISA. L'obiettivo è definire un insieme di funzioni più specifiche e aggiornate, così da supportare con

maggiore efficacia e tempestività l'impegno profuso dagli Stati membri, dalle istituzioni dell'Unione e dagli altri soggetti coinvolti nel garantire la sicurezza del ciberspazio europeo.

La proposta di direttiva mira a stabilire procedure e condizioni che aiutino a rendere più semplice il rispetto degli obblighi in materia di sicurezza informatica, favorendone un'applicazione più coerente ed efficace. Le modifiche apportate alla direttiva NIS 2 hanno lo scopo di semplificare la conformità e garantire un'attuazione razionalizzata e coerente di alcuni elementi specifici del quadro di cibersicurezza. Per questi motivi, la Commissione **ritiene necessario** un **intervento normativo**.

La valutazione di impatto

La valutazione di impatto (disponibile solo in lingua inglese; una sintesi è disponibile in italiano) elaborata dalla Commissione europea **analizza** tre **opzioni** di intervento per le **quattro aree principali** di intervento.

Il mandato dell'ENISA

Opzione A.1: chiarimento del mandato dell'Agenzia e definizione delle priorità attraverso l'integrazione dei suoi compiti stabiliti da altri atti legislativi dell'UE;

Opzione A.2: **riforma** del **mandato** dell'**ENISA** da realizzare attraverso l'abrogazione e la sostituzione del regolamento sulla cibersicurezza;

Opzione A.3: riforma del mandato dell'ENISA, come previsto dall'opzione precedente, e rafforzamento del sostegno operativo diretto ai singoli soggetti in caso di incidenti.

Il quadro europeo di certificazione della cibersicurezza

Opzione B.1: chiarimento dell'ambito di applicazione, degli elementi e degli obiettivi e introduzione di un nuovo meccanismo di mantenimento per i sistemi adottati;

Opzione B.2: **riforma** del **quadro** con **revisione** delle **procedure** ed **estensione** del suo **ambito di applicazione** per agevolare la conformità normativa;

Opzione B.3: riforma del quadro come previsto dall'opzione precedente e introduzione di una certificazione obbligatoria per la postura di cibersicurezza.

Semplificazione della conformità

Opzione C.1: adozione di strumenti non legislativi e non vincolanti per garantire un livello più elevato di armonizzazione di talune misure di gestione dei rischi di cibersicurezza, nonché delle informazioni e delle procedure di notifica;

Opzione C.2: **modifiche mirate** alla direttiva **NIS 2** per chiarire alcune definizioni, ridurre l'ambito di applicazione, introdurre la massima armonizzazione per gli atti di esecuzione;

Opzione C.3: armonizzazione totale delle misure relative alla cibersicurezza mediante l'eliminazione delle misure di gestione include nella normativa settoriale per centralizzarle all'interno della direttiva NIS 2.

Sicurezza delle catene di approvvigionamento TIC

Opzione D.1: adozione di un approccio basato su strumenti non vincolanti aumentando il numero di valutazioni coordinate del rischio e di pacchetti di strumenti volontari;

Opzione D.2: intervento normativo mirato mediante la codificazione del pacchetto di strumenti per il 5G e l'introduzione dell'obbligo per gli Stati membri di provvedere affinché nelle risorse chiave della rete non siano utilizzati componenti di fornitori ad alto rischio;

Opzione D.3: istituzione di un **quadro normativo** orizzontale, **neutro** dal punto di vista tecnologico e **settoriale**, per **affrontare i rischi di cibersicurezza** di natura non tecnica nelle catene di approvvigionamento.

L'impatto dell'opzione prescelta

La Commissione ha selezionato il **pacchetto strategico** composto dalle opzioni **A.2**, **B.2**, **C.2** e **D.3**.

Costi

La valutazione di impatto stima che le opzioni di intervento prescelte determineranno **costi**, nell'arco dei cinque anni successivi al momento dell'adozione delle proposte, pari a **circa 160 milioni di euro** per l'**ENISA**, a fronte dei suoi nuovi compiti, e di **80 milioni** per le attività di vigilanza delle **autorità pubbliche** in tutta l'UE. Inoltre, l'eliminazione graduale delle apparecchiature ad alto rischio dovrebbe comportare costi annui compresi **tra i 3,4 e i 4,3 miliardi di euro** per gli **operatori di reti mobili** e **spese aggiuntive** fino a **2 miliardi** di euro l'anno in **investimenti** in fornitori affidabili a carico delle imprese.

Benefici

La Commissione europea stima che il pacchetto dovrebbe determinare **risparmi** sui costi **fino a 15,3 miliardi di euro**, in un arco temporale di cinque anni, dovuti alla riduzione degli obblighi di conformità. Allo stesso modo, il miglioramento complessivo del livello di cibersicurezza e di sovranità tecnologica produrrà vantaggi rilevanti per gli Stati membri, le imprese e i cittadini dell'UE sul lungo periodo.

Coerenza con il quadro giuridico dell'UE

La revisione del regolamento sulla cibersicurezza è concepita per **integrare** la direttiva relativa alla resilienza dei soggetti critici (*c.d.* **direttiva CER**), che inserisce

considerazioni relative alla catena di approvvigionamento tra i pilastri per la resilienza dei soggetti critici. Tale revisione si coordinerebbe, inoltre, con una serie di interventi legislativi futuri, tra i quali:

- l'**atto legislativo** sullo **sviluppo del *cloud* e dell'IA**, che sarà presentato nel secondo semestre dell'anno, finalizzato, tra i vari obiettivi, a colmare la carenza di un'offerta competitiva di servizi di *cloud computing* a livello dell'Unione che sia adeguata, per dimensioni e capacità, a gestire settori o scenari d'uso ad alta criticità;
- la proposta di **regolamento sulle reti digitali** presentata nel gennaio 2026;
- la futura **revisione del regolamento sui *chip***;
- Il **quadro normativo sugli appalti pubblici**, con specifico riferimento alle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE (attualmente in fase di valutazione);
- la già menzionata proposta di regolamento per la semplificazione legislativa (all'interno del pacchetto ***omnibus* digitale**), che prevede l'obbligo per l'ENISA di istituire un p**unto di accesso unico per la segnalazione degli incidenti** attraverso il quale i soggetti possano adempiere contemporaneamente agli obblighi di segnalazione degli incidenti previsti da molteplici atti giuridici.

Il processo di revisione punterebbe anche a consolidare il ruolo delle autorità e degli operatori europei nelle interlocuzioni con i **partner del Mediterraneo meridionale**. L'obiettivo centrale è incentivare l'interconnessione tramite infrastrutture digitali caratterizzate da sicurezza e affidabilità nell'intero bacino mediterraneo, in linea con le priorità stabilite dal Patto per il Mediterraneo.

Parallelamente, sia la **Strategia europea** per l'**Unione della preparazione**, sia la Strategia europea di sicurezza interna (***ProtectEU***), hanno collocato la difesa cibernetica come pilastro fondamentale per la resilienza dell'UE. Tali documenti programmatici riconoscono che le continue minacce *cyber* non costituiscono meramente delle sfide di natura tecnica, bensì dei veri e propri pericoli strategici per le istituzioni democratiche, il sistema economico e il modello sociale europeo.

Allo stesso modo, la comunicazione sul **rafforzamento della sicurezza economica dell'UE** individua tra gli obiettivi principali la protezione di informazioni e dati sensibili che potrebbero compromettere la sicurezza economica dell'Unione e la prevenzione e il contrasto alle perturbazioni delle **infrastrutture critiche** europee che hanno ripercussioni sull'economia UE. In tali settori, l'adozione di protocolli di cibersicurezza efficienti riveste una funzione determinante.

La necessità di affrontare le perturbazioni delle catene di approvvigionamento e gli attacchi informatici è stata sottolineata anche nella strategia per l'Unione della preparazione e nel Libro bianco sulla **prontezza alla difesa europea per il 2030**. All'interno della strategia *ProtectEU*, la Commissione ha inoltre evidenziato come l'adozione di un approccio armonizzato per la sicurezza degli approvvigionamenti nel

settore delle TIC possa rappresentare la soluzione all'attuale frammentazione del mercato unico, derivante dalle differenti strategie nazionali. Tale coerenza permetterebbe di scongiurare dipendenze strategiche e di proteggere le filiere produttive delle TIC dai fornitori ad altro rischio, garantendo così la resilienza delle infrastrutture critiche.

La consultazione dei portatori di interessi

La Commissione informa di aver **consultato** i **portatori di interessi** mediante molteplici attività, tra cui:

- un **invito a presentare contributi** aperto dall'11 aprile al 20 giugno 2025;
- una **consultazione pubblica** condotta attraverso un sondaggio volto a valutare l'efficacia del quadro legislativo vigente;
- una serie di **interviste** con rappresentanti dell'ENISA, autorità pubbliche nazionali incaricate della gestione delle piattaforme di segnalazione ed esperti di certificazione;
- **consultazioni** ad alto livello **con gli Stati membri**, anche in sede di Consiglio presso i gruppi di lavoro;
- la raccolta di **pareri tecnici**, in particolare dall'*European Cybersecurity Certification Group* (ECCG) e dallo *Stakeholder Cybersecurity Certification Group* (SCCG);
- l'organizzazione di due ***workshop***, uno sui punti di forza e di debolezza identificati per l'ENISA e il quadro di certificazione, l'altro volto alla raccolta di suggerimenti;
- la commissione di uno **studio** a supporto della valutazione dell'ENISA e del ECCF.

Complessivamente, i portatori di interesse hanno sottolineato la necessità di **potenziare** il finanziamento dell'**ENISA** e chiarire che le attività di certificazione e il supporto alla cooperazione e all'attuazione delle politiche siano le priorità fondamentali del suo mandato. In relazione all'**ECCF**, la maggior parte degli intervistati si è dichiarato **insoddisfatto** dei **tempi necessari** allo sviluppo e all'adozione dei sistemi di certificazione, nonché per la mancanza di trasparenza e di coinvolgimento dei portatori di interesse nei processi decisionali.

Infine, la Commissione europea riporta che è stata espressa l'esigenza di ridurre la complessità degli obblighi e di affrontare i rischi derivanti dalla dipendenza da fornitori di Paesi terzi.

Principali contenuti delle proposte

Proposta di regolamento

La proposta consta di **122 articoli,** ripartiti in 5 titoli, e di 3 allegati.

Titolo I – Disposizioni generali

Il Titolo I della proposta di regolamento contiene le **disposizioni generali**.

L'articolo 1 stabilisce l'**oggetto** e l'**ambito di applicazione** del regolamento, precisando che lascia impregiudicate le funzioni essenziali degli Stati membri, tra cui la garanzia dell'integrità territoriale, il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza nazionale, che restano di competenza esclusiva di ciascuno Stato.

L'articolo 2 riporta le **definizioni** che si applicano al regolamento, compresi i riferimenti alle pertinenti definizioni di altri strumenti dell'Unione, quali la direttiva NIS 2, il regolamento che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e il regolamento sulla normazione europea.

Titolo II – Agenzia dell'Unione europea per la cibersicurezza

Il Titolo II contiene le **disposizioni fondamentali** relative all'**ENISA**. Il titolo è ripartito in sei capi.

Capo I - Missione e obiettivi

L'articolo 3 definisce quale **missione** dell'Agenzia dell'UE per la cibersicurezza sostenere gli Stati membri e i soggetti dell'Unione nel conseguimento di un livello elevato di cibersicurezza, di resilienza e di fiducia all'interno dell'Unione. A tal fine, l'ENISA dovrebbe fungere da punto di riferimento per consulenze e competenze in materia di cibersicurezza, contribuendo alla riduzione della frammentazione del mercato interno.

L'articolo 4 definisce gli **obiettivi** dell'ENISA, che si possono ricondurre a **quattro ambiti chiave** della cibersicurezza a livello unionale:

- assistere la Commissione nell'elaborazione delle politiche e della normativa in materia di cibersicurezza e, allo stesso tempo, sostenere gli Stati membri nell'attuazione uniforme di tale normativa, fornendo assistenza operativa agli Stati, alle istituzioni, organi e organismi dell'UE, e ai soggetti appartenenti ai settori pubblico e privato nel costante miglioramento delle loro capacità in termini di preparazione, resilienza e risposta;
- contribuire alla cooperazione operativa a livello dell'Unione, tra gli Stati membri, e a una maggiore condivisione della conoscenza situazionale in merito alle minacce e agli incidenti informatici tra gli Stati membri, soggetti UE e portatori di interesse pubblici e privati. Per migliorare la preparazione in materia di cibersicurezza e la risposta a incidenti di *ransomware*, è prevista la cooperazione dell'ENISA con Europol, i CSIRT e le altre autorità nazionali competenti;
- assicurare la certificazione della cibersicurezza e la normazione;
- realizzare l'Accademia per le competenze in materia di cibersicurezza, che dovrebbe contribuire allo sviluppo di una forza lavoro europea dinamica nel settore della cibersicurezza con competenze che dovrebbero essere trasferibili in tutti gli Stati membri.

Capo II - Compiti

Al Capo II sono illustrati i **compiti** dell'**Agenzia**, che si articolano in tre sezioni.

La **sezione 1** contiene disposizioni relative ai compiti connessi al sostegno dell'attuazione delle politiche e del diritto dell'Unione.

Con l'articolo 5, si individuano i **soggetti** e le **organizzazioni** che **devono ricevere sostegno** e le modalità con le quali tale sostegno dovrebbe realizzarsi. Per facilitare un'attuazione coerente ed efficace dell'*acquis* dell'Unione in materia di cibersicurezza, l'ENISA dovrebbe pubblicare orientamenti tecnici e relazioni, fornire consulenza e migliori pratiche e agevolare lo scambio di migliori pratiche tra le autorità competenti. Al fine di promuovere la cooperazione tra il settore pubblico e il settore privato e all'interno di quest'ultimo, in particolare per sostenere la protezione delle infrastrutture critiche, l'ENISA dovrebbe altresì sostenere la condivisione delle informazioni intra e intersettoriale, in particolare nei settori individuati come ad alta criticità o come settori critici negli allegati I e II della direttiva NIS 2, e delle informazioni relative ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del regolamento sui requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali. Di particolare interesse è la previsione che l'ENISA, nell'ambito del suo mandato, assista gli Stati membri e i soggetti pertinenti dell'Unione nello sviluppo e nella promozione di politiche sulla cibersicurezza che sostengano la disponibilità generale e l'integrità del carattere pubblico di una rete internet aperta.

Nel **parere adottato** il 18 marzo 2026, ai sensi dell'articolo 42 paragrafo 2 del regolamento sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, il **Comitato europeo per la protezione dei dati** (EDPB) e il **Garante europeo della protezione dei dati** (EDPS) raccomandano di **aggiungere** anche l'**EDPS** come **possibile richiedente** ai sensi dell'articolo 5, paragrafo 1, lettera *h)*, della proposta di regolamento, in considerazione del suo ruolo di autorità di controllo per il trattamento dei dati personali da parte di istituzioni, organi e agenzie dell'Unione europea. L'EDPB e l'EDPS sostengono fermamente che tale parere sia fornito solo previa richiesta dell'EDPB o, come proposto, dell'EDPS, così da garantire un chiaro coordinamento e una chiara divisione delle responsabilità con ENISA.

L'articolo 6 definisce le **responsabilità** dell'**ENISA** in materia di **sviluppo delle capacità**, tra cui l'offerta di conoscenze e competenze agli Stati membri in materia di prevenzione e contrasto delle minacce informatiche, l'aggiornamento delle strategie di cibersicurezza e l'espansione della forza lavoro nel settore della cibersicurezza.

L'articolo 7 prevede che l'ENISA **assista** gli **Stati membri** nelle loro **attività di sensibilizzazione**, effettuando, ai sensi dell'articolo 8, analisi delle principali tendenze del mercato in materia di cibersicurezza e diffondendo consulenze e analisi tecniche.

L'articolo 9 attribuisce all'ENISA l'impegno a contribuire al **dialogo** con i **paesi terzi** e le **organizzazioni internazionali**, per promuovere una cooperazione internazionale sulle questioni connesse alla cibersicurezza.

La **sezione 2** definisce i compiti dell'ENISA per quanto riguarda la **cooperazione operativa**.

In particolare, l'articolo 10 definisce con maggiore dettaglio tale cooperazione operativa in relazione agli Stati membri, ai soggetti dell'Unione e al servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione (CERT-UE), alla rete di CSIRT, alla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) e ad altri portatori di interessi, compresa la pubblicazione di orientamenti e l'attuazione di strumenti di comunicazione sicura.

In base all'articolo 11, l'ENISA dovrà contribuire inoltre a migliorare la **conoscenza situazionale** condivisa in materia di minacce e incidenti informatici, sviluppando tra l'altro, in cooperazione anche con Europol, uno o più archivi di *intelligence* sulle minacce informatiche, effettuando analisi ed emettendo allerte precoci in caso di incidente significativo o su vasta scala, potenziale o in corso, o di minaccia informatica di potenziale natura transfrontaliera.

Nel loro parere il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati hanno **richiesto chiarimenti** alla Commissione europea in merito agli articoli 10 e 11 della proposta. Ai sensi di questi articoli, infatti, l'ENISA amplierebbe il proprio ruolo di centro nevralgico per la cooperazione operativa, includendo l'elaborazione di ingenti quantità di informazioni di intelligence sulle minacce, che potrebbero includere dati personali, come indirizzi IP, credenziali utente, registri utente, transazioni finanziarie o dettagli di account compromessi. La Commissione europea ha tuttavia informato i due soggetti richiedenti che la proposta **non intende imporre né autorizzare** alcun **trattamento su larga scala** di dati personali da parte dell'ENISA. Alcuni controlli di cibersicurezza creano tuttavia rischi specifici per la protezione dei dati. Questo può essere il caso del monitoraggio e della registrazione, dell'ispezione approfondita dei pacchetti o dell'analisi del comportamento degli utenti. Un sistema di certificazione ben progettato per la sicurezza del trattamento dovrebbe includere controlli per garantire che le misure di sicurezza possano essere attuate in modo conforme alle norme sulla protezione dei dati. Occorre inoltre sottolineare che alcuni controlli possono proteggere la *privacy* e la protezione dei dati fin dalla progettazione ("*by design*") e per impostazione predefinita ("*by default*").

Le norme relative a tali allerte precoci (contenuto, tempistica, servizio) sono stabilite all'articolo 12.

Secondo le modalità esposte all'articolo 13 e, a seconda dei casi, in cooperazione con Europol e i CSIRT o altre autorità competenti, l'ENISA gestisce la **riserva dell'UE per la cibersicurezza**, allo scopo di assistere i soggetti essenziali e importanti nella preparazione e nella risposta agli incidenti di *ransomware*, nonché nella ripresa dagli stessi. A tal fine, l'ENISA **istituisce un *helpdesk*** apposito.

L'articolo 14 contiene disposizioni sul ruolo dell'ENISA nelle esercitazioni di cibersicurezza a livello dell'Unione, compresa l'elaborazione di un programma continuo annuale di esercitazioni di cibersicurezza a livello dell'Unione.

L'articolo 15 stabilisce che l'ENISA dovrebbe altresì istituire, fornire, gestire, mantenere e aggiornare, se necessario, **strumenti tecnici operativi**, comprese le piattaforme relative alla cibersicurezza a livello dell'Unione, nonché **strumenti di prova** a sostegno dell'attuazione delle **procedure di valutazione della conformità** a norma della pertinente normativa dell'Unione.

Il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati ricordano, nel citato parere, l'importanza di **garantire** la **sicurezza delle notifiche inviate** e trasmesse **attraverso** il **punto di accesso unico**, poiché le notifiche di violazione dei dati personali spesso includono informazioni sensibili.

Infine, in base all'articolo 16, l'Agenzia deve sviluppare una capacità comune di servizi per la gestione delle vulnerabilità dell'Unione e fornire servizi di gestione delle vulnerabilità ai portatori di interessi.

La **sezione 3**, dedicata alla **certificazione della cibersicurezza e alla normazione**, definisce i compiti dell'Agenzia a tale riguardo.

L'articolo 17 descrive il ruolo dell'ENISA nello sviluppo e nell'attuazione del quadro europeo di certificazione della cibersicurezza, compreso il suo **ruolo guida** nella preparazione e **diffusione** dei **sistemi** adottati – pubblicando in un apposito sito web le informazioni sui sistemi europei di certificazione della cibersicurezza, sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità – e nel garantirne il mantenimento nonché nello sviluppo delle capacità.

L'articolo 18 stabilisce in che modo l'ENISA dovrebbe impegnarsi nell'elaborazione di specifiche tecniche e orientamenti a sostegno dell'attuazione della normativa dell'Unione nel settore della cibersicurezza e dovrebbe, al contempo, contribuire alle attività di normazione a livello europeo e internazionale, anche nel settore degli algoritmi crittografici.

La **sezione 4** illustra in dettaglio i compiti dell'Agenzia per quanto riguarda la realizzazione dell'**Accademia per le competenze in materia di cibersicurezza**.

L'articolo 19 contiene disposizioni relative al ruolo dell'ENISA per quanto riguarda il quadro europeo delle competenze in materia di cibersicurezza (*European cybersecurity skills framework* – ECSF).

Nel parere il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati **raccomandano** ai colegislatori di emendare l'articolo 19, paragrafo 2, della proposta, in modo che l'**ECSF non sia limitato esclusivamente ai "professionisti della cibersicurezza"**, ma includa anche profili per la forza lavoro in generale, come i cittadini, i dipendenti pubblici o i lavoratori non specializzati. Tuttavia, il considerando 45 della proposta distingue esplicitamente il ECSF dal Quadro europeo delle competenze digitali (DigComp 3.0), chiarendo che quest'ultimo è destinato alla vita quotidiana e alla partecipazione alla società, al lavoro e all'apprendimento e può essere utilizzato sia dagli adulti che dai bambini, mentre l'ECSF è rivolto a un pubblico specializzato, offrendo un quadro semplice che identifica i ruoli in materia di sicurezza informatica e i relativi compiti, conoscenze e competenze necessari per svolgerli.

L'articolo 20 definisce i **compiti** dell'ENISA relativi **adozione** e **mantenimento** di **sistemi europei di attestazione delle competenze individuali** in materia di

cibersicurezza. Lo stesso articolo prevede che l'uso di sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza è volontario per gli organismi pubblici nazionali e i soggetti privati, salvo non sia diversamente stabilito dal diritto nazionale

L'articolo 21 individua i **requisiti** per diventare un **fornitore autorizzato di attestati europei** delle competenze individuali in materia di cibersicurezza.

L'articolo 22 contiene le prescrizioni relative all'esame delle domande per diventare fornitore autorizzato di attestati e mantenimento delle autorizzazioni.

L'articolo 23 prevede che l'ENISA metta a disposizione del pubblico e aggiorni regolarmente un apposito sito *web* che fornisce informazioni pubbliche riguardanti, tra l'altro, l'ECSF, sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza, il costo indicativo di un attestato europeo delle competenze individuali, i progressi compiuti e le tempistiche per il loro sviluppo.

Capo III - Organizzazione dell'ENISA

Il Capo III riguarda l'**organizzazione** dell'**ENISA** ed è suddiviso in 7 sezioni.

L'articolo 24 definisce la **struttura amministrativa** e di gestione dell'ENISA.

La **sezione 1** (articoli a 25 a 29) è dedicata al **consiglio di amministrazione**: l'articolo 25 stabilisce la sua composizione, l'articolo 26 è dedicato alla figura del presidente e del vicepresidente, mentre l'articolo 27 alle riunioni del consiglio di amministrazione. Gli articoli 28 e 29 stabiliscono, rispettivamente, le funzioni e le modalità di voto.

La **sezione 2** (articolo 30) detta la disciplina del **comitato esecutivo**, che svolge funzioni di assistenza al consiglio di amministrazione.

La **sezione 3** comprende le norme relative al **direttore esecutivo**.

L'articolo 31 si disciplina le modalità di nomina, rimozione dall'incarico e proroga del mandato del direttore esecutivo.

L'articolo 32 definisce i compiti e le responsabilità. In particolare, si stabilisce che il direttore esecutivo è indipendente nello svolgimento dei suoi compiti e non sollecita né accetta istruzioni da alcun governo o altro organismo. In base alle esigenze e nell'ambito degli obiettivi e dei compiti dell'ENISA, il direttore esecutivo può tra l'altro istituire gruppi di lavoro ad hoc composti da esperti, anche inviati dalle autorità competenti degli Stati membri. Il direttore esecutivo può inoltre essere invitato dal Parlamento europeo o dal Consiglio a riferire sullo svolgimento dei suoi compiti.

La **sezione 4** riguarda la figura del **vicedirettore esecutivo**.

L'articolo 33 stabilisce che il consiglio di amministrazione può decidere di creare una funzione di vicedirettore esecutivo per assistere il direttore esecutivo.

In base all'articolo 34, il vicedirettore esecutivo assiste il direttore esecutivo nella gestione dell'ENISA e nello svolgimento dei compiti di cui all'articolo 32.

La **sezione 5**, composta dal solo articolo 35, è dedicata al **gruppo consultivo ENISA**, istituito dal consiglio di amministrazione, su proposta del direttore esecutivo, con l'obiettivo di fornire consulenza all'ENISA e di garantire un dialogo regolare con il settore privato e altri soggetti interessati. Tale gruppo è composto da esperti riconosciuti che rappresentano i portatori di interessi appartenenti, tra gli altri, ai settori della cibersicurezza, al settore delle

TIC, le PMI, i soggetti che operano nei settori individuati come ad alta criticità o come settori critici negli allegati I e II della direttiva NIS 2, i fabbricanti di prodotti con elementi digitali e i gestori di software open source i soggetti che operano nel settore dei mezzi di identificazione elettronica, le organizzazioni dei consumatori, gli esperti del mondo accademico nel settore della cibersicurezza, le organizzazioni europee di normazione, nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.

La **sezione 6** stabilisce le norme relative alla **commissione di ricorso**.

L'articolo 36 riguarda la creazione e la composizione della commissione di ricorso. In base a questo articolo, il consiglio di amministrazione nomina il presidente, gli altri membri e i loro supplenti in base a un elenco di candidati idonei predisposto dalla Commissione e valido per un periodo di quattro anni.

L'articolo 37 definisce la durata del mandato dei membri della commissione di ricorso e dei loro supplenti, la loro indipendenza e le modalità di rimozione dall'incarico.

L'articolo 38 specifica le circostanze in cui i membri della commissione di ricorso devono astenersi dal prendere parte a un procedimento di ricorso e illustra i motivi per cui un membro della commissione può essere ricusato.

In base all'articolo 39, si può presentare ricorso presso la commissione di ricorso avverso le decisioni prese dall'ENISA o in caso di suo mancato intervento. Il paragrafo 3 stabilisce che tale ricorso non ha effetto sospensivo.

L'articolo 40 contiene disposizioni sulle persone legittimate a presentare ricorso, sui termini e sulla forma del ricorso.

Gli articoli da 41 a 43 disciplinano la revisione precontenziosa, l'esame delle decisioni sui ricorsi e i ricorsi dinanzi alla Corte di giustizia.

Infine, la **sezione 7**, composta dal solo articolo 44, regola il processo di adozione del documento unico di programmazione, che contiene il programma di lavoro annuale e pluriennale e include tutte le attività pianificate

Capo IV - Formazione e struttura del bilancio dell'ENISA

Il Capo IV riguarda: la **formazione del bilancio** dell'ENISA (articolo 45), la **struttura** del bilancio (articolo 46), i diritti riscossi da ENISA nell'ambito del sistema europeo di attestazione e di valutazione della conformità, con lo scopo di contribuire a coprire integralmente i costi dello svolgimento delle proprie attività (articolo 47), l'esecuzione del bilancio (articolo 48), la rendicontazione e il discarico (articolo 49) e la regolamentazione finanziaria (articolo 50).

L'articolo 51 contiene anche le disposizioni per facilitare la **lotta contro la frode**, la **corruzione** e altre attività illecite.

L'articolo 52 regola la dichiarazione, resa dai membri del consiglio di amministrazione, dal direttore esecutivo, dal vicedirettore esecutivo, come pure dai funzionari distaccati dagli Stati membri a titolo temporaneo, con la quale indicano l'assenza o la presenza di interessi diretti o indiretti che possano essere considerati in contrasto con la loro indipendenza.

L'articolo 53 è dedicato alla **trasparenza** che deve caratterizzare le attività di ENISA, accompagnata dall'obbligo di riservatezza delle informazioni trattate (articolo 54).

Conclude il capo l'articolo 55 relativo al regime di accesso ai documenti, definito dal regolamento relativo all'accesso del pubblico ai documenti

Capo V - Personale e funzionari di collegamento

Il Capo V riguarda il **personale dell'Agenzia** e comprende disposizioni generali relative allo statuto dei funzionari e al regime applicabile agli altri agenti (articolo 56), nonché le regole che disciplinano i privilegi e le immunità (articolo 57).

L'articolo 58 introduce disposizioni che impongono agli Stati membri di designare almeno due funzionari di collegamento dell'autorità nazionale competente quali esperti nazionali distaccati presso l'ENISA definendone il ruolo in seno all'Agenzia.

L'articolo 59 consente ad ENISA il ricorso a esperti nazionali distaccati e ad altro personale non alle dipendenze dell'Agenzia.

Capo VI - Disposizioni generali relative all'ENISA

Il Capo VI contiene le **disposizioni generali** relative all'Agenzia.

L'articolo 60 ne definisce lo ***status* giuridico**, ossia un organismo dell'Unione con personalità giuridica.

L'articolo 61 stabilisce che l'Agenzia ha sede ad Atene (Grecia).

L'articolo 62 contiene disposizioni concernenti l'accordo sulla sede e le condizioni operative dell'Agenzia.

L'articolo 63 stabilisce che il Mediatore europeo vigila sull'operato dell'ENISA conformemente all'articolo 228 del TFUE.

Gli articoli da 64 a 67 includono disposizioni che disciplinano le questioni di responsabilità contrattuale, extracontrattuale e del personale dell'Agenzia (articolo 64), il regime linguistico (articolo 65) e la protezione dei dati personali (articolo 66), nonché le norme di sicurezza in materia di protezione delle informazioni sensibili non classificate e di quelle classificate (articolo 67).

Nel citato parere, il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (EDPS) hanno ritenuto che, qualora i futuri compiti dell'ENISA in qualità di centro di informazione richiedessero un trattamento sostanziale dei dati personali, ciò dovrebbe essere esplicitamente indicato nelle disposizioni dell'atto costitutivo che disciplina i rispettivi compiti, compresi gli elementi essenziali di qualsiasi trattamento su larga scala e le opportune garanzie. Viceversa, se l'obiettivo è quello di consentire all'ENISA di raccogliere e trattare principalmente dati non personali aggregati, anche questo aspetto dovrebbe essere chiarito. Preoccupazioni per l'EDPB e l'EDPS ha destato anche il paragrafo 2 dell'articolo 66, laddove stabilisce che il consiglio di amministrazione può adottare misure aggiuntive necessarie per l'applicazione del regolamento (UE) 2018/1725 da parte dell'ENISA, non specificando la portata, procedura applicabile e la tipologia di tali misure aggiuntive. Un tale intervento, poiché interferisce con i diritti fondamentali, dovrebbe essere riservato al legislatore o, al massimo, alla Commissione tramite atti di esecuzione o delegati. In ogni caso le misure adottate dal Consiglio di amministrazione dovrebbero essere chiare e precise, la loro applicazione

prevedibile per le persone interessate, attraverso un'adeguata pubblicità, nonché assicurare il rispetto dei principi e delle garanzie fondamentali in materia di protezione dei dati.

Gli articoli da 68 a 70 stabiliscono norme per la cooperazione dell'ENISA con i soggetti dell'Unione e le autorità nazionali (articolo 68), con altri portatori di interessi (articolo 69) e con i Paesi terzi e le organizzazioni internazionali (articolo 70).

Titolo III – Quadro europeo di certificazione della cibersicurezza

Il Titolo III istituisce il **quadro europeo di certificazione della cibersicurezza** ed è composto da 3 capi.

Capo I - Obiettivi, ambito di applicazione e procedure

Il Capo I introduce gli **obiettivi**, l'**ambito di applicazione** e le **procedure** del quadro europeo di certificazione della cibersicurezza.

L'articolo 71 definisce gli obiettivi e l'ambito di applicazione del quadro europeo. Gli obiettivi comprendono il **rafforzamento della cibersicurezza** in tutta l'Unione e l'agevolazione di un approccio armonizzato alla certificazione dei prodotti, dei servizi e dei processi relativi alle tecnologie TIC, dei servizi di sicurezza gestiti o della postura di cibersicurezza dei soggetti. A tal fine il quadro dovrebbe aumentare il livello di cibersicurezza all'interno dell'Unione e rendere possibile un approccio armonizzato ai sistemi europei di certificazione della cibersicurezza, facendo inoltre leva sulla certificazione per agevolare il rispetto della normativa applicabile dell'Unione. Lo stesso articolo stabilisce inoltre che la **certificazione** europea della cibersicurezza **è volontaria**, salvo sia diversamente specificato nel diritto dell'Unione o nazionale, e che il certificato europeo di cibersicurezza e la dichiarazione UE di conformità rilasciati nell'ambito del quadro europeo di certificazione della cibersicurezza sono automaticamente riconosciuti in tutti gli Stati membri.

L'articolo 72 illustra poi gli **aspetti procedurali**, a cominciare dalle consultazioni sulle priorità strategiche in materia di certificazione europea della cibersicurezza e dalla pubblicazione delle informazioni relative all'elaborazione del sistema da parte della Commissione, nonché dalla creazione di una nuova assemblea europea sulla certificazione della cibersicurezza.

L'articolo 73 stabilisce che, a seguito di una richiesta dettagliata della Commissione, l'ENISA dovrebbe presentare una proposta di un sistema europeo di certificazione della cibersicurezza per i prodotti, i servizi e dei processi TIC, i servizi di sicurezza gestiti o la postura di cibersicurezza dei soggetti.

L'articolo 74 prevede che entro 12 mesi dal ricevimento di una richiesta della Commissione a norma dell'articolo 73, salvo diversamente specificato nella richiesta, l'ENISA prepara una proposta di sistema europeo di certificazione della cibersicurezza. Per la preparazione di ciascuna proposta di sistema, l'ENISA istituisce un gruppo di lavoro *ad hoc* in conformità dell'articolo 32, il cui scopo è fornire all'ENISA una consulenza specialistica. In sede di preparazione della proposta di sistema, l'ENISA coopera

strettamente con gruppo europeo per la certificazione della cibersicurezza (ECCG). L'ECCG fornisce all'ENISA assistenza e consulenza specialistica in relazione alla preparazione della proposta di sistema e, ove applicabile, delle relative specifiche tecniche. In sede di preparazione della proposta di sistema e, ove applicabile, delle relative specifiche tecniche, l'ENISA consulta tempestivamente i portatori di interessi mediante un processo di consultazione formale, aperto, trasparente e inclusivo, cooperando inoltre con le autorità pubbliche competenti degli Stati membri e con i pertinenti soggetti dell'Unione. In sede di adozione o riesame di un regime, la Commissione può includere riferimenti alle specifiche tecniche individuate ai sensi degli articoli 18 e 77.

L'articolo 75 afferma che ciascun sistema europeo di certificazione della cibersicurezza deve definire una **strategia di mantenimento dello stesso**.

L'articolo 76, disciplina la **valutazione**, **revisione** e **ritiro** di un **sistema europeo** di **certificazione** della cibersicurezza. Il riesame di un sistema potrebbe basarsi inoltre su una valutazione periodica della sua efficacia e del suo impatto sul mercato unico.

L'articolo 77 fornisce all'ENISA una base per elaborare specifiche tecniche a sostegno dello sviluppo e del mantenimento dei sistemi europei di certificazione della cibersicurezza. Le varie procedure garantiscono la trasparenza e la qualità dei risultati coinvolgendo esperti e comuni portatori di interessi nelle varie fasi della pianificazione, dello sviluppo, dell'adozione e del mantenimento dei sistemi di certificazione.

L'articolo 78 stabilisce che, se un atto giuridico specifico dell'Unione lo prevede, un **certificato rilasciato** nell'ambito di un sistema europeo di certificazione della cibersicurezza **dimostra la conformità** e **conferisce** una **presunzione di conformità** alle corrispondenti prescrizioni di tale atto giuridico, riducendo in tal modo gli oneri per le imprese.

L'articolo 79 prevede un apposito sito *web* dell'ENISA sui **sistemi europei** di **certificazione della cibersicurezza**, che dovrebbe fornire informazioni, tra l'altro, sui sistemi adottati, nonché sui certificati europei di cibersicurezza e sulle dichiarazioni UE di conformità rilasciati nell'ambito di tali sistemi.

Capo II - Contenuto dei sistemi europei di certificazione della cibersicurezza

Il Capo II stabilisce le **norme generali** per il **contenuto** dei **sistemi europei di certificazione della cibersicurezza**.

L'articolo 80 stabilisce un elenco di obiettivi di sicurezza dei sistemi europei di certificazione della cibersicurezza che devono essere rispettati dal sistema progettato dall'ENISA e garantisce l'allineamento alla normativa pertinente in materia di cibersicurezza.

Nel parere del 18 marzo scorso il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati raccomandano di chiarire ulteriormente l'**ambito di applicazione** dell'articolo 80, paragrafo 1, lettera w) della proposta e il suo rapporto con il regolamento GDPR, in particolare laddove gli schemi si applichino a prodotti, servizi, processi TIC e servizi di sicurezza gestiti che potrebbero essere utilizzati nelle operazioni di trattamento dei dati. Inoltre, è opportuno distinguere la certificazione in materia di

sicurezza informatica dalla certificazione in materia di protezione dei dati, prevista con un'apposita procedura dagli articoli 42 e 43 del regolamento GDPR.

L'articolo 81 specifica elementi, regole e condizioni che ciascun sistema europeo di certificazione della cibersicurezza deve e può prevedere. Tali caratteristiche devono essere compatibili con la normativa dell'Unione e possono essere armonizzate tra i vari sistemi ricorrendo a principi comuni e disposizioni tipo, adottati dalla Commissione europea con appositi atti di esecuzione

L'articolo 82 disciplina i **livelli di affidabilità** e la **valutazione** dei **sistemi europei** di certificazione della cibersicurezza. I livelli di affidabilità sono ripartiti in "di base", "sostanziale" o "elevato". Tali livelli di affidabilità sono **commisurati** al **livello di rischio associato** all'uso del prodotto, del servizio TIC e processo TIC o al servizio di sicurezza gestito, o – in termini di probabilità e impatto di un incidente – alla natura dei soggetti la cui postura di cibersicurezza è oggetto di certificazione e al loro ambiente operativo. Sono poi definiti i requisiti di sicurezza associati a ciascun livello.

L'articolo 83 stabilisce che un sistema europeo di certificazione della cibersicurezza può consentire **un'autovalutazione della conformità** sotto la **sola responsabilità del fabbricante o del fornitore** di prodotti, servizi e processi TIC o servizi di sicurezza gestiti o del soggetto la cui postura di cibersicurezza è oggetto di certificazione.

L'articolo 84, infine, fornisce un elenco di informazioni supplementari che il fabbricante o fornitore di prodotti, servizi o processi TIC deve mettere a disposizione dell'utente.

Capo III - Governance del quadro europeo di certificazione della cibersicurezza

Il Capo III stabilisce le **norme di *governance*** per il quadro europeo di certificazione della cibersicurezza, suddivise in tre sezioni.

La **sezione 1** contiene le **disposizioni generali** per la gestione dei sistemi europei di certificazione della cibersicurezza.

L'articolo 85 disciplina le **modalità di rilascio** di certificati europei di cibersicurezza.

L'articolo 86 stabilisce le **norme per l'armonizzazione** dei sistemi europei di certificazione della cibersicurezza con i sistemi nazionali di certificazione della cibersicurezza e i certificati di cibersicurezza nazionali. Ai sensi di questo articolo, I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti, i servizi, i processi e i soggetti che rientrano nell'oggetto e nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato dalla Commissione europea. sulla base della proposta di sistema preparata dall'ENISA. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate che non rientrano nell'oggetto e nell'ambito di applicazione di un sistema europeo di certificazione della cibersicurezza possono restare in vigore.

L'articolo 87 prevede la possibilità di riconoscimento internazionale dei certificati europei di cibersicurezza, sulla base del **principio di equivalenza**, mediante un atto di esecuzione adottati dalla Commissione o attraverso la conclusione di un accordo tra

l'Unione e il paese terzo in questione o un'organizzazione internazionale, a condizione di reciprocità.

L'articolo 88 definisce inoltre il **ruolo delle autorità nazionali** di certificazione della cibersicurezza e le relative norme applicabili, stabilendo, tra l'altro, che ciascuna autorità nazionale di certificazione della cibersicurezza è indipendente dai soggetti sui quali vigila per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale. Inoltre, le attività delle autorità nazionali di certificazione della cibersicurezza relative al rilascio di certificati europei di cibersicurezza dovranno essere rigorosamente separate e indipendenti dalle attività di vigilanza. L'articolo in esame riconosce anche specifici poteri che devono essere assegnati a ciascuna autorità nazionale di certificazione della cibersicurezza, come condurre indagini, sotto forma di *audit* o accesso ai locali, nei confronti degli organismi di valutazione della conformità, dei titolari dei certificati europei di cibersicurezza e degli emittenti di dichiarazioni UE di conformità e irrogare sanzioni, nel rispetto della legislazione dell'Unione o del diritto nazionale.

L'articolo 89 stabilisce le norme per un **meccanismo di revisione tra pari** tra le autorità nazionali di certificazione della cibersicurezza, garantendo un'applicazione delle norme equivalente in tutta l'Unione,

L'articolo 90 istituisce il **gruppo europeo per la certificazione della cibersicurezza** (ECCG), composto da rappresentanti delle autorità nazionali di certificazione della cibersicurezza o da rappresentanti di altre autorità nazionali competenti. Tra i compiti assegnati, l'ECCG consiglia e coadiuva la Commissione nelle sue attività volte a garantire un'attuazione e un'applicazione coerenti delle disposizioni, nelle questioni relative alla politica in materia di certificazione della cibersicurezza e nel coordinamento degli approcci strategici, nonché assiste, consiglia e collabora con l'ENISA.

La **sezione 2** disciplina gli **organismi di valutazione della conformità**.

L'articolo 91 definisce la competenza degli organismi di valutazione della conformità.

L'articolo 92 prevede un'ulteriore armonizzazione della competenza degli organismi di valutazione della conformità.

L'articolo 93 contiene norme in materia di notifica, compreso il conferimento di poteri alla Commissione europea di adottare atti di esecuzione per stabilire le circostanze, i formati e le procedure per le notifiche al fine di garantire un ulteriore allineamento al pertinente diritto dell'Unione e al nuovo quadro legislativo.

L'articolo 94 disciplina una procedura di contestazione che garantisca il rispetto dei requisiti per gli organismi di valutazione della conformità.

L'articolo 95 stabilisce specifici obblighi di informazione e conservazione a carico degli organismi di valutazione della conformità.

La **sezione 3**, composta da due articoli, prevede all'articolo 96 il diritto di **presentare** un **reclamo** e il diritto a un **ricorso giurisdizionale** effettivo in relazione al rilascio improprio, al mancato rilascio o al riconoscimento di un certificato europeo di cibersicurezza.

L'articolo 97 impone agli Stati membri di stabilire e applicare **sanzioni proporzionate**, **effettive** e **dissuasive** in caso di violazioni della regolamentazione.

Titolo IV – sicurezza delle catene di approvvigionamento delle TIC

Il Titolo IV contiene disposizioni relative alla **sicurezza** delle **catene di approvvigionamento** delle TIC. Il titolo in esame si articola in 3 capi.

Capo I - Quadro per catene di approvvigionamento delle TIC affidabili

L'articolo 98 definisce l'**ambito di applicazione** del quadro per catene di approvvigionamento delle TIC affidabili. Il quadro prevede un meccanismo di sicurezza a livello dell'Unione volto ad affrontare i rischi di natura non tecnica nei settori ad alta criticità e in altri settori critici di cui alla direttiva NIS 2. Il meccanismo individua le **risorse TIC chiave nelle catene di approvvigionamento critiche** e stabilisce misure di attenuazione adeguate e proporzionate al tipo di soggetti appartenenti ai settori ad alta criticità e in altri settori critici elencati negli allegati I e II della direttiva NIS 2. Gli Stati membri possono adottare o mantenere disposizioni che garantiscano un livello più elevato di cibersicurezza nelle catene di approvvigionamento delle TIC, a condizione che tali disposizioni siano coerenti con i loro obblighi stabiliti dal diritto dell'Unione.

L'articolo 99 specifica in che modo le **valutazioni dei rischi per la sicurezza saranno effettuate**, precisando che dovrebbero anche stabilire **misure di attenuazione**. La Commissione o un gruppo di almeno tre Stati membri può chiedere al gruppo di cooperazione gruppo di cooperazione NIS, istituito dall'articolo 14 della direttiva NIS 2, di effettuare a livello dell'Unione valutazioni coordinate dei rischi per la sicurezza. Tali valutazioni coordinate dei rischi devono essere completate entro sei mesi dalla richiesta. Su richiesta della Commissione, il gruppo di cooperazione NIS può concordare un periodo più breve. Il quadro prevede altresì la possibilità di una procedura di emergenza se un intervento immediato è giustificato per preservare il buon funzionamento del mercato interno e qualora la Commissione abbia motivi sufficienti per ritenere che sussista una minaccia informatica significativa per la sicurezza dell'Unione in relazione alle catene di approvvigionamento critiche delle TIC. In tal caso, la Commissione consulta gli Stati membri sulla necessità di adottare una o più misure di attenuazione ed effettua una valutazione dei rischi. La valutazione dei rischi per la sicurezza comprende la proposta identificazione delle risorse TIC chiave, nonché dei principali autori delle minacce, dei rischi e delle vulnerabilità che interessano tali risorse. Nell'ambito della valutazione dei rischi per la sicurezza sono poi elaborati scenari di rischio e sono proposte misure per attenuare i rischi individuati.

L'articolo 100 stabilisce che se, a seguito della valutazione dei rischi di cui all'articolo 99 o sulla base di altre fonti, come una dichiarazione pubblica a nome dell'Unione o di uno Stato membro, risulta che un paese terzo presenta rischi gravi e strutturali di natura non tecnica per le catene di approvvigionamento delle TIC, la **Commissione europea verifica la minaccia** rappresentata da tale paese, tenendo conto di una serie di elementi elencati direttamente dall'articolo 100, come ad esempio obblighi di informazione in caso di vulnerabilità di *software* o *hardware* o l'assenza di mezzi di ricorso giurisdizionali efficaci e di meccanismi di controllo indipendente e democratico in materia di sicurezza. Qualora la Commissione **concluda che un paese terzo presenta rischi gravi e strutturali di natura**

non tecnica per le catene di approvvigionamento delle TIC, l'articolo 100 prevede una procedura che consente alla Commissione di **designare**, mediante un atto di esecuzione, tale paese terzo come **paese che desta preoccupazioni per la cibersicurezza** delle catene di approvvigionamento delle TIC. I **soggetti stabiliti in un paese terzo che desta preoccupazioni** per la cibersicurezza a norma di questo articolo, o controllati da tale paese terzo, da un soggetto ivi stabilito o da un suo cittadino, **non saranno autorizzati a svolgere una serie di attività** specificate in tale articolo, tra le quali partecipare alle fasi di elaborazione, valutazione o consultazione, alle decisioni riguardanti le norme europee e i prodotti della normazione europea e alle procedure di appalto pubblico.

L'articolo 101 prevede un meccanismo generale per la sicurezza delle catene di approvvigionamento delle TIC in base al quale, una volta completata la valutazione dei rischi per la sicurezza da parte del gruppo di cooperazione NIS o della Commissione a norma dell'articolo 99, la Commissione può adottare le misure di cui agli articoli 102 e 103.

L'articolo 102 attribuisce alla Commissione il potere di adottare atti di esecuzione per individuare le risorse TIC chiave utilizzate per la fabbricazione di prodotti e la fornitura di servizi da parte dei tipi di soggetti appartenenti ai settori ad alta criticità e in altri settori critici elencati negli allegati I e II della direttiva NIS 2. Questo articolo specifica ulteriormente gli elementi da prendere in considerazione per l'individuazione delle risorse TIC chiave.

L'articolo 103 stabilisce **possibili misure di attenuazione** nella catena di approvvigionamento delle TIC, per garantire un livello elevato di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione. La Commissione può infatti decidere, mediante atti di esecuzione, di imporre nei confronti dei soggetti che operano in settori ad alta criticità e in altri settori critici determinate misure di attenuazione, ulteriormente specificate nell'articolo, tra le quali anche il divieto di utilizzare, installare o integrare in qualsiasi forma nelle risorse TIC chiave componenti TIC o componenti che comprendono componenti TIC di fornitori ad alto rischio, anche stabiliti in un paese terzo o controllati da un paese terzo, che rappresenti un rischio di cibersicurezza di natura non tecnica significativo per le attività economiche o sociali di almeno tre Stati membri.

L’articolo 104 prevede che la Commissione, mediante atti di esecuzione, stila **elenchi di fornitori ad alto rischio** pertinenti ai fini dei divieti stabiliti nell'articolo 103 e nel successivo articolo 111, dopo aver anche svolto una valutazione del luogo di stabilimento e dell'assetto proprietario e di controllo. La Commissione, nello svolgimento di tale esame, dovrebbe consultare i fornitori interessati e le autorità competenti, che possono essere chiamate a effettuare una valutazione preliminare del luogo di stabilimento e dell'assetto proprietario e di controllo di un fornitore.

L'articolo 105 disciplina la **richiesta** – e la relativa procedura – di **esenzione** per i **soggetti stabiliti in un paese terzo che desta preoccupazioni** per la cibersicurezza o controllati da soggetti di tale paese terzo. Tali soggetti possono infatti chiedere di essere autorizzati a fornire componenti TIC destinati a risorse TIC chiave di soggetti appartenenti ai settori individuati come ad alta criticità e in altri settori critici dagli allegati I e II della direttiva NIS 2 e a partecipare agli appalti pubblici in relazione alla fornitura di tali componenti TIC. La Commissione valuta tale richiesta tramite un processo equo e

trasparente, prendendo in considerazione circostanze ed elementi individuati dallo stesso articolo. Essa conclude la propria procedura di esame della richiesta entro nove mesi dal ricevimento della richiesta con l'adozione di una decisione notificata al richiedente, che, in caso di esito favorevole, può contenere talune limitazioni temporali o condizioni cui il soggetto deve attenersi.

L'articolo 106 specifica i diritti della difesa del soggetto richiedente l'esenzione di cui al precedente articolo.

L'articolo 107 attribuisce alla Commissione l'obbligo di tenere un registro accessibile al pubblico delle decisioni relative alle esenzioni.

Gli articoli 108 e 109 specificano le norme in materia di riservatezza e i diritti riscossi dalla Commissione relativamente alla richiamata procedura di esenzione.

Capo II - Catene di approvvigionamento delle TIC nelle reti di comunicazione elettronica

Il Capo II prevede l'**applicazione** del **quadro per catene di approvvigionamento delle TIC** affidabili alle reti di comunicazione elettronica mobili, fisse e satellitari, garantendo l'allineamento all'atto legislativo sulle reti digitali.

L'articolo 110 rimanda all'allegato II della proposta per l'individuazione delle risorse TIC chiave per le reti di comunicazione elettronica mobili, fisse e satellitari. Il periodo di transizione per l'eliminazione graduale dei componenti TIC di fornitori ad alto rischio per le risorse TIC chiave della rete di comunicazione elettronica mobile non supera i 36 mesi dall'entrata in vigore del presente regolamento. I periodi transitori per le reti di comunicazione elettronica fisse e satellitari sono specificati dalla Commissione mediante atti di esecuzione. Alla Commissione è conferito il potere di adottare atti delegati per modificare le risorse TIC chiave designate e i periodi transitori, anche per le future generazioni di reti mobili.

L'articolo 111 stabilisce che i fornitori di reti di comunicazione elettronica mobili, fisse e satellitari non possono utilizzare, installare o integrare, in alcuna forma, componenti TIC di fornitori ad alto rischio nell'ambito delle risorse TIC chiave.

Capo III - Autorità competenti, vigilanza ed esecuzione, giurisdizione, diritti della difesa

Il Capo III stabilisce **norme dettagliate** in materia di **autorità competenti**, **vigilanza**, **esecuzione** e **giurisdizione**.

L'articolo 112 stabilisce che **ciascuno Stato membro designa** le **autorità competenti** di cui all'articolo 8 della direttiva NIS 2 quali autorità responsabili dell'adozione delle misure di vigilanza e di esecuzione di cui al successivo articolo 114. Per l'Italia, l'autorità competente NIS è l'**Agenzia per la cybersicurezza nazionale** (ACN). Tale articolo richiede che le autorità competenti siano pienamente **imparziali**, a livello strutturale e funzionale, e non subiscono alcuna influenza esterna, diretta o indiretta; in particolare non sollecitano né accettano istruzioni da altre autorità pubbliche o da privati.

L'articolo 113 prevede che, ai fini di una vigilanza efficace, la Commissione istituisca una **rete di cooperazione** tra le autorità competenti degli Stati membri e la Commissione. Tale rete ha il compito di fungere da **piattaforma per la cooperazione e lo scambio di informazioni**, in particolare ai fini della valutazione del luogo di stabilimento e dell'assetto proprietario e di controllo ai sensi dell'articolo 104.

L'articolo 114 specifica le **misure di vigilanza** e di **esecuzione** che **le autorità competenti** sono **autorizzate ad adottare.** Tra queste: richieste di accesso a dati, documenti e informazioni necessari per verificare la conformità al presente regolamento; ispezioni in loco e vigilanza a distanza; adozione di decisioni che impongono ai soggetti interessati di porre rimedio alla violazione del presente regolamento o alle carenze individuate nell'attuazione delle misure di attenuazione; imposizione di sanzioni o richiesta di l'imposizione di sanzioni da parte degli organismi o degli organi giurisdizionali pertinenti, conformemente al diritto nazionale. Nell'adottare queste misure di esecuzione, le autorità competenti devono tenere debitamente conto di una serie di elementi elencati dal medesimo articolo. Le autorità competenti, nell'esercizio delle citate attività, rispettano il principio di riservatezza e il principio del segreto professionale e commerciale.

L'articolo 115 attribuisce agli Stati membri l'adozione delle norme relative alle **sanzioni da applicare** in caso di violazione del futuro regolamento, adottando tutte le misure necessarie per assicurarne l'applicazione. Lo stesso articolo individua alcune modalità di calcolo della sanzione, commisurate al totale del fatturato mondiale annuo relativo all'esercizio precedente, ripartite in base al tipo di violazione posta in essere.

L'articolo 116 contiene disposizioni dettagliate in merito alla possibilità per gli Stati membri di **assistersi reciprocamente** quando i soggetti svolgono attività transfrontaliere o quando le loro risorse TIC chiave sono situate in più Stati membri. In base a questo articolo, 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. Se opportuno e di comune accordo le autorità competenti di diversi Stati membri possono svolgere le attività di vigilanza congiunte.

L'articolo 117 stabilisce le **norme in materia di competenza giurisdizionale e territorialità**, prevedendo anche modalità per l'individuazione della giurisdizione con riferimento a specifiche categorie di soggetti.

Titolo V – Disposizioni finali

Si segnala che nel testo dell'articolato il Titolo risulta come Titolo VI a causa di un errore di numerazione.

Il Titolo V comprende **disposizioni finali**

L'articolo 118 stabilisce che la Commissione, nell'adozione degli atti esecutivi, è assistita da un comitato che si riunisce in due formazioni. Per quanto riguarda i titoli II e III,

la Commissione è assistita dal comitato riunito nella prima formazione; per quanto riguarda il titolo IV la Commissione è invece assistita dal comitato riunito nella seconda formazione. Per i casi disciplinati da questo paragrafo si applica l'articolo 5 del regolamento (UE) n. 182/2011 che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (*c.d.* Comitologia). L'articolo 5, in particolare, disciplina la procedura d'esame.

L'articolo 119 definisce le modalità con le quali la Commissione può adottare atti delegati.

L'articolo 120, stabilisce che ogni cinque anni, la Commissione esegue una valutazione di una serie di elementi, tra i quali le prestazioni dell'ENISA in relazione ai suoi obiettivi, al suo mandato, alla sua missione, ai suoi compiti, alla sua governance e alla sua ubicazione e l'efficacia, l'efficienza e il valore aggiunto dell'UE dei sistemi europei di attestazione delle competenze individuali in materia di cibersicurezza. La Commissione riferisce al Parlamento europeo, al Consiglio e al consiglio di amministrazione sui risultati della valutazione, che comunque sono resi pubblici.

L'articolo 121 dispone l'abrogazione del regolamento sulla cibersicurezza stabilendo altresì tutti i riferimenti presenti in tale regolamento, relativi all'ENISA e ai sistemi europei di certificazione della cibersicurezza istituiti dal regolamento sulla cibersicurezza, si dovranno intendere riferiti al futuro regolamento.

L'articolo 122 fissa la data di **entrata in vigore** del regolamento nel giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'UE.

Proposta di direttiva

La proposta consta di **4 articoli** e 1 allegato.

L'**articolo 1** prospetta modifiche alla direttiva NIS 2 finalizzate alla **semplificazione** di aspetti specifici del quadro in materia di cibersicurezza, ad aumentare la **certezza del diritto** e all'**armonizzazione** della sua attuazione.

In particolare, il punto 1), lettera a), modifica l'articolo 2, paragrafo 2, eliminando dall'**ambito di applicazione** della direttiva i fornitori di servizi di sistema dei nomi di dominio e aggiungendo i fornitori di portafogli europei di identità digitale e i fornitori di portafogli europei delle imprese.

La Commissione europea ha presentato la proposta di regolamento che istituisce i portafogli europei delle imprese nell'ambito del settimo pacchetto di semplificazione (v. dossier RUE). Presso la Camera, in esito all'esame ai fini della verifica della conformità al principio di sussidiarietà, la Commissione Politiche dell'UE ha adottato, il 24 febbraio 2026, un documento recante una **valutazione conforme** sulla proposta.

Inoltre, la lettera b) inserisce il paragrafo 3 *bis* che estende l'ambito di applicazione ai proprietari, gestori e operatori di **infrastrutture strategiche** a **duplice uso** a norma della proposta di regolamento sulla mobilità militare presentata dalla Commissione europea nel

novembre 2025 (v. dossier RUE) per includere tutti i gestori di infrastrutture sottomarine di trasmissione dati in considerazione dei crescenti rischi connessi a tali infrastrutture.

Presso la Camera, in esito all'esame ai fini della verifica della loro conformità al principio di sussidiarietà, la Commissione Politiche dell'UE ha adottato, il 4 marzo 2026, un documento recante una **valutazione conforme** sulla proposta.

Il punto 2), lettera a), interviene sull'articolo 3, paragrafo 1, introducendo la categoria delle piccole imprese a media capitalizzazione (***small mid-caps***) e i fornitori di cui al punto 1) tra i **soggetti** considerati **essenziali** ai fini della direttiva.

La categoria si *small mid-caps* è introdotta in linea con la raccomandazione del 21 maggio 2025 della Commissione europea.

La lettera b) modifica il paragrafo 4 per specificare i dati minimi che i soggetti devono comunicare alle autorità per la compilazione dell'elenco dei soggetti essenziali ed importati definito dagli Stati membri ai sensi del paragrafo 3 dello stesso articolo.

Il punto 3) modifica l'articolo 5 inserendo il **principio** della **massima armonizzazione** per quanto riguarda gli atti di esecuzione adottati a norma dell'articolo 21, paragrafo 5, della direttiva come modificato dalla presente proposta. In particolare, si prevede che gli Stati membri non possono imporre requisiti tecnici, metodologici o settoriali aggiuntivi se la Commissione europea ha già legiferato su tali aspetti tramite atti di esecuzione (v. *infra*).

Il punto 4) modifica l'articolo 6 relativo alle definizioni per aggiungere i concetti di *small mid-caps* e di infrastruttura sottomarina di trasmissioni dei dati.

Il punto 5) interviene sull'articolo 7 al fine di obbligare gli Stati membri a includere, nell'ambito della loro **strategia nazionale per la cibersicurezza**, politiche per la migrazione verso la **crittografia *post-quantum***.

Il punto 6) modifica l'articolo 15, paragrafo 2, per formalizzare la partecipazione dell'ENISA ai team di risposta agli incidenti di sicurezza informatica (CSIRT).

Il punto 7), lettera a), modifica l'articolo 21, paragrafo 5, secondo comma, prevedendo che la Commissione valuti periodicamente se gli atti di esecuzione in relazione alle misure di gestione dei rischi di cibersicurezza debbano essere adottati per settori o tipi di soggetti specifici, concentrandosi in particolare sulla natura transfrontaliera e svolgendo un processo di consultazione con i portatori di interesse e gli Stati membri. La lettera b) prevede invece l'aggiunta di un ulteriore comma per introdurre l'**obbligo** a carico degli **Stati membri** di **non imporre ulteriori requisiti** ai soggetti che rientrano nell'ambito di applicazione degli atti di esecuzione della Commissione, qualora questi siano stati adottati.

Il punto 8) aggiunge all'articolo 23 il paragrafo 12 che prevede che nell'adozione di un atto di esecuzione che specifichi il tipo di informazioni, il formato e la procedura di trasmissione di una notifica su eventuali incidenti che hanno un impatto significativo sulla fornitura dei servizi, la Commissione vi deve includere l'**obbligo** di **segnalare** alcune specifiche informazioni relative agli **attacchi *ransomware***. Viene inserito anche il paragrafo 13 per prevedere che, in caso di incidente significativo causato da *ransomware*, gli Stati membri provvedano affinché i soggetti interessati comunichino se è stata ricevuta una **richiesta di riscatto** e se è stato pagato tale riscatto anche il corrispettivo **importo**, il **mezzo di pagamento** e il **destinatario**.

Vista la sensibilità dei dati segnalati e in linea con i principi di necessità e proporzionalità, qualora la segnalazione di attacchi *ransomware* comporti il trattamento di dati personali, nel parere del 18 marzo 2026 il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati raccomandano di specificare nell'atto di esecuzione, ai sensi dell'articolo 23, paragrafo 12, della direttiva NIS2, le garanzie applicabili in materia di protezione dei dati.

Il punto 9) modifica l'articolo 24 al fine di prevedere che, per dimostrare la conformità alle misure di gestione dei rischi di cibersicurezza, gli Stati membri possono imporre ai soggetti essenziali e importanti di ottenere un **certificato** sulla **postura di cibersicurezza** nell'ambito del sistema europeo di certificazione come regolato dall'articolo 75 del regolamento sulla cibersicurezza riveduto nell'ambito della proposta parallela del presente pacchetto in esame. Nel caso in cui tale certificazione sia posseduta, le autorità competenti **non devono sottoporre** il soggetto a **misure di vigilanza supplementari** rispetto ai requisiti certificati.

Il punto 10) modifica l'articolo 26 per chiarire che i vettori aerei sono considerati, ai sensi dell'applicazione della presente direttiva, sotto la giurisdizione dello Stato membro la cui autorità competente per il rilascio delle licenze ha rilasciato la licenza d'esercizio a norma del regolamento recante norme comuni per la prestazione di servizi aerei.

Il punto 11) prevede che l'ENISA debba creare e mantenere un **registro dei soggetti** essenziali e importanti e dei soggetti che forniscono servizi di registrazione dei nomi di dominio sulla base delle informazioni ricevute dai punti di contatto unici.

Il punto 12) prevede l'aggiunta del nuovo articolo 37 *bis* che disciplina il **ruolo** di **assistenza** dell'**ENISA**, che dovrà, tra le altre cose, assistere gli Stati membri nello svolgimento delle attività di assistenza reciproca di cui all'articolo 37 della direttiva.

L'articolo 37 prevede che nel caso in cui un soggetto fornisca servizi in più di uno Stato membro le autorità competenti degli Stati interessati debbano cooperare e assistersi reciprocamente in funzione delle necessità.

Il punto 13) dispone che gli allegati I e II della direttiva NIS 2 siano modificati in conformità all'allegato della presente direttiva.

L'**articolo 2** regola i **termini di recepimento** dell'atto prevedendo che entro i dodici mesi successivi all'entrata in vigore dello stesso, gli Stati membri adottano le misure legislative, regolamentari e amministrative necessarie per conformarsi, informandone la Commissione europea.

Gli **articoli 3** e **4** disciplinano l'**entrata in vigore**, nel ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'UE, e i **destinatari** (gli Stati membri) della direttiva.

Coerenza con i principi dei trattati in materia di competenza dell'UE

Base giuridica

La base giuridica di **entrambe le proposte** è costituita dall'**articolo 114** del trattato sul funzionamento dell'Unione europea (TFUE), in coerenza con gli atti che sono intesi modificare, ai sensi del quale il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, possono adottare le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno.

Sussidiarietà

La Commissione europea sostiene che la **conformità** delle due proposte al **principio di sussidiarietà** in ambito di cibersicurezza **è stata già accertata** con **l'adozione** sia del **regolamento sulla cibersicurezza** attualmente in vigore, sia al momento dell'**adozione della direttiva NIS 2**. La natura transfrontaliera delle minacce informatiche rende infatti indispensabile un'azione coordinata a livello UE. L'attuale frammentazione derivante dalla coesistenza di sistemi di certificazione e approcci normativi nazionali differenti genera oneri burocratici e penalizza la competitività del mercato unico.

Si **rende pertanto necessario** un **quadro giuridico** dell'Unione **aggiornato**, capace di superare tali ostacoli e garantire un'applicazione omogenea delle regole. Poiché la sicurezza informatica costituisce un **interesse strategico comune**, tale **obiettivo non è pienamente raggiungibile dai singoli Stati membri**, richiedendo necessariamente un intervento a livello europeo.

Proporzionalità

La Commissione ritiene che le misure proposte siano **strettamente limitate** a **quanto occorre** per **raggiungere** gli **obiettivi strategici** individuati. L'intervento dell'UE, inoltre, non preclude ai singoli Stati la possibilità di adottare ulteriori provvedimenti a tutela della sicurezza nazionale. Per quanto concerne il quadro europeo di certificazione della cibersicurezza, la certificazione conserva natura volontaria, fungendo da strumento per attestare la conformità ai requisiti di cibersicurezza dell'Unione. Tale impostazione, secondo la Commissione europea, assicura il **rispetto** del **principio di proporzionalità**. Per quanto riguarda la direttiva, la Commissione ritiene che le modifiche prospettate alla NIS 2 non vadano al di là di quanto necessario per il conseguimento degli obiettivi dell'intervento, quali l'allineamento e la razionalizzazione delle misure di sicurezza e degli obblighi di segnalazione.

Riguardo alla **scelta** dell'**atto giuridico**, osserva la necessità che la revisione del *Cybersecurity Act* avvenga mediante lo stesso strumento giuridico. Il processo di recepimento nel caso di una direttiva per questo tipo di intervento potrebbe infatti

lasciare un margine di discrezionalità eccessivo a livello nazionale, portando potenzialmente alla mancanza di uniformità di taluni requisiti essenziali di cibersicurezza, all'incertezza giuridica, a un'ulteriore frammentazione o addirittura a situazioni discriminatorie a livello transfrontaliero. La scelta dello strumento del regolamento è stata inoltre ricondotta anche all'esigenza di ridurre frammentazione e complessità, in coerenza con la proposta di regolamento sulle reti digitali (v. *supra*).

Nel caso della direttiva, la Commissione sostiene che la proposta è coerente con il testo giuridico che è inteso modificare e consente di mantenere in capo agli Stati membri la flessibilità necessaria per tenere conto delle specificità nazionali.

Esame presso le Istituzioni dell'UE

Le proposte sono esaminate secondo la **procedura legislativa ordinaria** e sono assegnate all'esame della Commissione per l'industria, la ricerca e l'energia (ITRE) del Parlamento europeo.

Esame presso altri parlamenti nazionali

Sulla base dei dati forniti dal sito IPEX, l'esame delle proposte risulta concluso dal Parlamento della Repubblica d'Irlanda e avviato dai Parlamenti di Finlandia, Lettonia e Svezia, dal *Bundesrat* tedesco e dal Senato ceco. Il solo esame della proposta di direttiva è stato avviato anche dal Senato polacco. **Nessuna** di tali assemblee ha segnalato al momento di aver individuato aspetti rilevanti o di avere informazioni importanti da scambiare.