Council of the European Union

Brussels, 13 May 2026
(OR. en, it)

9257/26

Interinstitutional Files:
2026/0011 (COD)
2026/0012 (COD)

CYBER 226
JAI 584
DATAPROTECT 158
TELECOM 233
MI 476
IND 335
CADREFIN 215
FIN 678
BUDGET 17
CSC 302
CODEC 909
INST 225
PARLNAT 121
PARLNAT

COVER NOTE

From:	President of the Italian Chamber of Deputies
date of receipt:	12 May 2026
To:	The President of the Council of the European Union
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) -[5611/26 - COM(2026) 11 final] Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2] -[5627/26 - COM(2026) 12 final] - Reasoned opinion on the application of the Principles of Subsidiarity and Proportionality

Delegations will find enclosed the opinion[1] of the Italian Chamber of Deputies on the above.

[1] The translation(s) of the opinion may be available on the Interparliamentary EU Information Exchange website (IPEX) at the following address: https://secure.ipex.eu/IPEXL-WEB/document/COM-2026-0011 https://secure.ipex.eu/IPEXL-WEB/document/COM-2026-0013

Doc. **XVIII-*bis***
n. 102

CAMERA DEI DEPUTATI

XIV COMMISSIONE
(POLITICHE DELL'UNIONE EUROPEA)

DOCUMENTO APPROVATO DALLA XIV COMMISSIONE NELL'AMBITO DELLA VERIFICA DI SUSSIDIARIETÀ DI CUI ALL'ARTICOLO 6 DEL PROTOCOLLO N. 2 ALLEGATO AL TRATTATO DI LISBONA:

PROPOSTA DI REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO RELATIVO ALL'AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA (ENISA), AL QUADRO EUROPEO DI CERTIFICAZIONE DELLA CIBERSICUREZZA E ALLA SICUREZZA DELLE CATENE DI APPROVVIGIONAMENTO DELLE TIC E CHE ABROGA IL REGOLAMENTO (UE) 2019/881 ("REGOLAMENTO SULLA CIBERSICUREZZA 2")
(COM(2026) 11 FINAL)

PROPOSTA DI DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO CHE MODIFICA LA DIRETTIVA (UE) 2022/2555 PER QUANTO RIGUARDA LE MISURE DI SEMPLIFICAZIONE E L'ALLINEAMENTO ALLA [PROPOSTA DI REGOLAMENTO SULLA CIBERSICUREZZA 2]
(COM(2026) 13 FINAL)

Approvato il 6 maggio 2026

DOCUMENTO APPROVATO DALLA COMMISSIONE

La XIV Commissione,

esaminate, ai fini della verifica di conformità con il principio di sussidiarietà, la Proposta di regolamento del Parlamento europeo e del Consiglio relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza delle catene di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881 ("regolamento sulla cibersicurezza 2") (COM(2026) 11) e la proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di semplificazione e l'allineamento alla [proposta di regolamento sulla cibersicurezza 2] (COM(2026) 13);

considerato il crescente rilievo della cibersicurezza quale componente essenziale dell'autonomia strategica e della sicurezza dell'Unione europea e degli Stati membri;

preso atto delle relazioni trasmesse dal Governo ai sensi dell'articolo 6, comma 5, della legge 24 dicembre 2012, n. 234, sulle proposte;

tenuto conto degli elementi di conoscenza e di valutazione emersi dalle memorie trasmesse da soggetti qualificati nell'ambito dell'esame delle proposte;

considerato che la Tabella di marcia "Un'Europa, un mercato unico" del Parlamento europeo, del Consiglio dell'UE e della Commissione europea prevede l'adozione delle proposte entro la fine del 2026;

premesso che:

- la valutazione delle finalità generali del pacchetto è complessivamente positiva, in linea con quanto sostenuto nella relazione del Governo, poiché si inserisce nel più ampio rafforzamento del quadro europeo di cibersicurezza;
- tale rafforzamento deve tuttavia garantire un equilibrio tra l'integrazione del mercato interno, da un lato, e la salvaguardia delle competenze degli Stati membri in materia di sicurezza, dall'altro;
- occorre in particolare garantire certezza giuridica, chiarezza nella *governance* e una netta delimitazione delle responsabilità operative tra livello nazionale e unionale;
- le proposte risultano di particolare urgenza alla luce del contesto geopolitico e tecnologico caratterizzato da un aumento della frequenza e della sofisticazione degli attacchi cyber;

rilevato, con riferimento al rispetto del principio di attribuzione, che la base giuridica su cui si fondano le proposte è correttamente costituita dall'articolo 114 del Trattato sul funzionamento dell'Unione europea (TFUE);

ritenute le proposte complessivamente conformi al principio di sussidiarietà, in quanto necessarie a regolare settori nei quali l'intervento a livello nazionale risulta insufficiente e poiché presentano un chiaro valore aggiunto, considerata la natura prettamente transfrontaliera della cibersicurezza;

permangono tuttavia specifici ambiti nei quali le misure prospettate dalle proposte in esame rischiano di risultare eccessivamente invasive rispetto al livello nazionale, con particolare riferimento alla dimensione operativa ed alla *governance* del sistema; in particolare, si rileva che:

per quanto riguarda la proposta di regolamento:

- pur essendo condivisibile in via generale il rafforzamento delle capacità di ENISA in termini di risorse umane e finanziarie, l'attribuzione all'Agenzia di funzioni operative, ai sensi degli articoli da 10 a 16, potrebbe determinare un'alterazione dell'equilibrio tra le autorità competenti a livello unionale e nazionale, nonché elementi d'incertezza nella gestione operativa degli incidenti;
- la possibilità per la Commissione europea di adottare sistemi europei di certificazione della cibersicurezza anche senza il parere favorevole delle autorità nazionali, come previsto dall'articolo 74, potrebbe ridurre il contributo decisionale degli Stati membri in un ambito strettamente connesso alla sicurezza nazionale e alla resilienza delle infrastrutture critiche;
- nonostante si riconosca l'opportunità d'istituire un quadro europeo minimo armonizzato per garantire la sicurezza della catena di approvvigionamento del mercato unico dell'UE, il trasferimento dal livello nazionale a quello europeo di funzioni strategiche, soprattutto in relazione alle tecnologie TIC (tecnologie dell'informazione e della comunicazione), di cui alle disposizioni del Titolo IV, rischia di limitare la capacità degli Stati membri di effettuare valutazioni autonome su profili tecnici, economici e di sicurezza nazionale;
- il riconoscimento alla Commissione europea della facoltà di definire, tramite atti di esecuzione, una lista di fornitori considerati ad alto rischio, ai sensi dell'articolo 104, postulerebbe la fissazione nel regolamento di criteri tecnici, trasparenti e verificabili, al fine di evitare valutazioni discrezionali suscettibili di incidere sul corretto funzionamento del mercato interno e sulla concorrenza;

per quanto riguarda la proposta di direttiva:

- il vigente obbligo di garantire l'applicazione integrale della direttiva NIS 2 anche a soggetti che non saranno più coinvolti ai sensi della medesima proposta potrebbe determinare effetti distorsivi nel mercato interno, penalizzando gli Stati membri, tra i quali l'Italia, che hanno già adempiuto integralmente agli obblighi di recepimento della direttiva;

considerata la proposta di regolamento solo parzialmente conforme al principio di proporzionalità in quanto:

- l'approccio nei confronti dei cosiddetti "fornitori ad alto rischio" rischia di introdurre una forma di discriminazione nel mercato digitale europeo, poiché le valutazioni sulla nazionalità, sulla struttura proprietaria, sul Paese di origine o su esposizioni a "influenze" potrebbero risultare non pienamente ancorate a criteri tecnici oggettivi, con il rischio di introdurre elementi di discriminazione nel mercato digitale europeo;
- l'eventuale esclusione di un fornitore ad alto rischio, in assenza di alternative equivalenti sul mercato, potrebbe alterare la concorrenza e determinare una concentrazione artificiale del mercato a favore di un numero ristretto di operatori;

- il rilevante impatto economico, peraltro in un orizzonte temporale limitato, potrebbe incidere non solo mediante una svalutazione degli investimenti già effettuati dalle imprese, bensì anche sulla loro capacità di investire in copertura e qualità del servizio;
- con specifico riferimento agli obblighi imposti per il settore delle reti di telecomunicazione, le tempistiche previste (36 mesi) ai fini della sostituzione dei componenti di fornitori ad alto rischio relativamente alle reti di comunicazione elettronica mobili, di cui all'articolo 110, sono più restrittive rispetto a quelle adottate nel contesto delle disposizioni relative al *golden power*, che peraltro si applicano alla sola componente della rete di accesso radio; inoltre, riguardo alla analoga sostituzione per le reti di comunicazione elettronica fisse e satellitari, si evidenzia l'ampia discrezionalità attribuita alla Commissione europea, che potrebbe generare incertezza giuridica;
- di fronte alla difficoltà tecnica di garantire l'assenza totale di vulnerabilità nei prodotti certificati, alcune imprese potrebbero essere obbligate a sostituire apparecchiature ancora funzionanti, determinando un aumento sostanziale degli oneri;

considerata la proposta di direttiva complessivamente conforme al principio di proporzionalità, come sostenuto anche dal Governo, in quanto non prevede misure ulteriori rispetto a quanto necessario a migliorare il quadro normativo vigente; si rilevano tuttavia:

- la necessità di esercitare il principio di proporzionalità previsto dall'articolo 21 della direttiva NIS 2, che consente di imporre obblighi più leggeri ai soggetti meno esposti ai rischi o con impatto potenzialmente limitato, invece di operare una completa esclusione degli stessi dall'ambito di applicazione della direttiva;
- l'assenza nella valutazione di impatto che accompagna la proposta di una specifica stima degli effetti di alcune misure previste, quali:
  a) l'esclusione dei soggetti attualmente compresi nel campo di applicazione della direttiva NIS 2 e i potenziali costi derivanti da incidenti di cibersicurezza che coinvolgono tali soggetti, che sarebbero sottoposti a obblighi differenziati;
  b) le conseguenze sulle attività delle autorità nazionali competenti a vigilare sul rispetto degli obblighi da parte dei soggetti esclusi, non essendo previste indicazioni per la fase transitoria relativa a tale modifica dell'ambito di applicazione della direttiva NIS 2;

rilevata inoltre l'esigenza di valutare accuratamente, nel corso dei negoziati interistituzionali, i seguenti aspetti, apportando le modifiche appropriate alle proposte originarie:

in riferimento a entrambe le proposte:

- la previsione di un raccordo formale e strutturato con gli strumenti di difesa cibernetica nell'ambito della Politica di Sicurezza e Difesa Comune (PSDC), al fine di garantire coerenza tra dimensione civile e militare della cibersicurezza e da condurre a un sistema europeo coerente;

per quanto riguarda la proposta di regolamento:

- il riconoscimento dei differenti impatti economici sui singoli mercati nazionali, prevedendo adeguati strumenti di supporto finanziario e industriale;

- l'introduzione di una clausola generale di salvaguardia che ribadisca il carattere non operativo dell'ENISA, evitando ogni sovrapposizione con le competenze delle autorità nazionali;
- la presenza di rigidità applicative che potrebbero penalizzare l'ecosistema industriale nazionale, anche rispetto ai compiti attribuiti all'ENISA, che vanno definiti in coerenza con i meccanismi di raccordo istituzionale già previsti da altri atti normativi europei vigenti in materia di cibersicurezza;
- l'introduzione di garanzie procedurali rigorose in merito al trattamento dei dati personali da parte di ENISA nell'esercizio delle attività operative previste dagli articoli 10 e 11;
- la limitazione ad una funzione puramente consultiva dell'*helpdesk* dell'ENISA per la preparazione e la risposta agli incidenti di *ransomware*, istituito ai sensi dell'articolo 13, o, in alternativa, l'esplicita precisazione che ENISA non gestisce incidenti né accede a dati sensibili degli Stati membri;
- il chiarimento delle condizioni d'intervento di ENISA nelle attività formative, di cui all'articolo 14, prevedendo il coinvolgimento delle autorità nazionali competenti ed introducendo altresì meccanismi di finanziamento adeguati, una programmazione pluriennale e una periodicità definita;
- il rafforzamento del ruolo strategico del consiglio di amministrazione di ENISA, di cui all'articolo 25 e seguenti, per garantire maggiore flessibilità nella rappresentanza degli Stati membri e l'introduzione di un principio di rotazione nelle nomine, prevedendo anche la possibilità per il Direttore esecutivo di delegare funzioni all'istituendo Vicedirettore;
- il rischio di trasferimento indiretto sulle PMI dei costi derivanti dalla riscossione dei diritti per il mantenimento dei sistemi di certificazione, previsti dall'articolo 47;
- la riduzione del distacco obbligatorio, previsto dall'articolo 58 della proposta, da due ad un solo funzionario di collegamento per Stato membro, prevedendo che i costi siano sostenuti dal bilancio di ENISA, limitando le attività di diffusione delle informazioni al solo Stato membro di appartenenza e definendo con chiarezza compiti e responsabilità;
- la necessità di evitare che la certificazione europea della cibersicurezza si trasformi da strumento volontario, come previsto dall'articolo 71, a requisito obbligatorio, favorendo gli operatori più grandi, che possono sostenere i costi della certificazione, a scapito di PMI e soggetti meno organizzati;
- la definizione nel dettaglio delle regole e delle specifiche tecniche per i sistemi di certificazione elaborate da ENISA per garantire la trasparenza dei processi decisionali e il coinvolgimento dei portatori di interesse;

per quanto riguarda la proposta di direttiva:

- riconsiderare l'esclusione di taluni soggetti dal campo di applicazione della direttiva NIS 2 in mancanza di una adeguata valutazione dei potenziali costi legati a futuri incidenti cyber, oppure, in alternativa, prevedere misure compensative per i soggetti che hanno già sostenuto investimenti legati alla direttiva NIS 2;

rilevata l'esigenza che il presente documento sia trasmesso al Parlamento europeo, al Consiglio e alla Commissione europea nell'ambito del dialogo politico,

VALUTA CONFORMI

le proposte al principio di sussidiarietà di cui all'articolo 5 del Trattato sull'Unione europea.