Consiglio dell'Unione europea

Bruxelles, 22 gennaio 2026
(OR. en)

5611/26
ADD 2

Fascicoli interistituzionali:
2026/0011 (COD)
2026/0012 (COD)

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	21 gennaio 2026
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	SWD(2026) 12 final
Oggetto:	DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO […] che accompagna i documenti 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") e 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]

Si trasmette in allegato, per le delegazioni, il documento SWD(2026) 12 final.

All.: SWD(2026) 12 final

COMMISSIONE
EUROPEA

Strasburgo, 20.1.2026
SWD(2026) 12 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO

[…]

che accompagna i documenti

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")

e

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) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Sintesi della valutazione d'impatto

Obiettivo

L'obiettivo principale della presente valutazione d'impatto è valutare l'adeguatezza delle normative vigenti nell'affrontare l'evoluzione delle minacce alla cibersicurezza in tutta l'UE. Propone una serie integrata di opzioni strategiche volte a rafforzare l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), a riformare il quadro europeo di certificazione della cibersicurezza (ECCF) e a semplificare la conformità al quadro normativo vigente in materia di cibersicurezza. La presente valutazione sottolinea l'importanza di modulare la governance informatica per allinearla ai progressi tecnologici e alle richieste del mercato, garantendo nel contempo la competitività e tenendo conto degli impatti ambientali.

Descrizione del problema

Nonostante gli sforzi in atto, il panorama della cibersicurezza dell'UE si trova ancora ad affrontare sfide significative in un contesto di minacce sempre più complesse. L'insufficiente coordinamento tra gli Stati membri e altri attori a livello dell'UE, lo stallo nell'attuazione degli strumenti strategici, gli ostacoli e la complessità normativa ostacolano una gestione efficiente della cibersicurezza. Tali problematiche si traducono in un aumento dei costi per le imprese e le autorità pubbliche, in un aumento dei rischi di incidenti informatici e in livelli incoerenti di protezione per i cittadini.

Giustificazione dell'azione dell'UE

Le minacce alla cibersicurezza trascendono i confini nazionali; pertanto un approccio unificato è essenziale per una risposta solida. Un intervento a livello dell'UE garantisce una protezione coerente, rafforza la competitività garantendo condizioni di parità e facilita la libera circolazione dei servizi e dei prodotti digitali all'interno del mercato unico. L'armonizzazione a livello dell'UE riduce inoltre gli oneri amministrativi attraverso la semplificazione della conformità e la razionalizzazione delle procedure.

Opzioni strategiche e opzione preferita

La presente relazione analizza quattro settori di intervento, ciascuno con una serie di opzioni strategiche considerate alla luce degli obiettivi specifici da conseguire: 1) il mandato dell'ENISA (già parte del regolamento sulla cibersicurezza vigente); 2) il quadro europeo di certificazione della cibersicurezza (già parte del regolamento sulla cibersicurezza vigente) e 3) modifiche mirate della direttiva NIS 2, il cui obiettivo è la semplificazione, ma che sono anche interconnesse con il mandato dell'ENISA e con il quadro europeo di certificazione della cibersicurezza. Ciascuna serie di opzioni rappresenta un settore di intervento a sé stante, pur essendo al contempo interconnessa e correlata alle altre.

Opzioni per affrontare il disallineamento tra il quadro strategico dell'UE in materia di cibersicurezza e le esigenze dei portatori di interessi in un contesto sempre più ostile

Opzione A.1: *chiarimento del mandato dell'ENISA e definizione delle priorità* – Questa opzione garantirebbe un quadro chiaro e stabile per i compiti dell'ENISA integrando i compiti stabiliti da altri atti legislativi.

Opzione A.2: *riforma del mandato dell'ENISA* – Questa opzione abrogherebbe e sostituirebbe il regolamento sulla cibersicurezza, prevedendo una revisione del mandato dell'Agenzia.

Opzione A.3: *riforma del mandato dell'ENISA con una forte attenzione al sostegno operativo* – Questa opzione si baserebbe sull'opzione A.2. Inoltre l'ENISA svilupperebbe le capacità per aiutare direttamente, su richiesta di uno Stato membro, i soggetti contemplati dalla direttiva NIS 2 nella risposta e nella ripresa in caso di incidenti di cibersicurezza.

Opzioni per il quadro europeo di certificazione della cibersicurezza

Opzione B.1: *chiarimento dell'ambito di applicazione, degli elementi e degli obiettivi del quadro europeo di certificazione della cibersicurezza e introduzione di un meccanismo di mantenimento* – Questa opzione prevedrebbe un nuovo meccanismo di mantenimento per i sistemi, dopo la loro adozione, che sarà attuato dall'ENISA.

Opzione B.2: *riforma del quadro europeo di certificazione della cibersicurezza rivedendone le procedure ed estendendo l'ambito di applicazione per agevolare la semplificazione della conformità normativa* – Con questa opzione, il regolamento sulla cibersicurezza sarebbe abrogato e sostituito da un nuovo regolamento. In aggiunta a quanto previsto dall'opzione B.1, sarebbe rivista anche la procedura relativa alla richiesta, allo sviluppo e all'adozione dei sistemi, per migliorare la rendicontabilità e l'efficienza.

Opzione B.3: *riforma del quadro europeo di certificazione della cibersicurezza come previsto dall'opzione B.2 e introduzione di una certificazione obbligatoria per la postura di cibersicurezza* – Questa opzione si baserebbe sull'opzione B.2, ma mira a potenziare ulteriormente l'impatto del quadro introducendo la certificazione obbligatoria per i soggetti essenziali rientranti nell'ambito di applicazione della direttiva NIS 2 tenendo conto di scenari di rischio specifici, invece di fare esclusivamente affidamento sulla certificazione volontaria dei soggetti.

Opzioni di semplificazione

Opzione C.1: *adozione di un approccio basato su strumenti non legislativi e non vincolanti, compreso il ricorso ai poteri esistenti (adozione di atti di esecuzione a norma dell'articolo 21, paragrafo 5, e dell'articolo 23, paragrafo 11, della direttiva NIS 2)* – Questa opzione prevede l'adozione di atti di esecuzione utilizzando i poteri esistenti a norma della direttiva NIS 2 per garantire un livello più elevato di armonizzazione delle misure di gestione dei rischi di cibersicurezza, delle soglie per la segnalazione degli incidenti, nonché delle informazioni, dei formati e della procedura delle notifiche, accompagnata dall'adozione di una serie di orientamenti volti a rafforzare la certezza del diritto e ad armonizzare l'attuazione.

Opzione C.2: *intervento mirato: ulteriore semplificazione della conformità al pertinente quadro normativo dell'Unione in materia di cibersicurezza* – Questa opzione comporta un intervento limitato attraverso modifiche del regolamento sulla cibersicurezza e della direttiva

NIS 2 con l'obiettivo di semplificare aspetti specifici del quadro in materia di cibersicurezza, tra cui adeguamenti dell'ambito di applicazione, massima armonizzazione per gli atti di esecuzione, prova della conformità attraverso la certificazione, e adozione della serie di orientamenti previsti dall'opzione C1.

Opzione C.3: *armonizzazione delle misure relative alla cibersicurezza stabilite nella normativa dell'Unione* – Questa opzione si baserebbe sull'opzione C.2 e eliminerebbe tutte le misure di gestione dei rischi di cibersicurezza o i poteri conferiti in relazione a tali misure previsti nella normativa settoriale. L'ecosistema della direttiva NIS 2 sarebbe invece modificato per prevedere obblighi semplificati per tutti i tipi di soggetti, garantendo in tal modo una maggiore armonizzazione.

Opzioni per la sicurezza delle catene di approvvigionamento delle TIC

Opzione D.1: *adozione di un approccio non vincolante per affrontare i rischi di cibersicurezza per le catene di approvvigionamento delle TIC* – Questa opzione non prevedrebbe un intervento normativo a livello dell'UE. La Commissione aumenterebbe invece il numero di valutazioni coordinate del rischio e di pacchetti di strumenti volontari.

Opzione D.2: *Intervento normativo ad hoc che codifica il pacchetto di strumenti per il 5G* – Questa opzione codificherebbe le misure del pacchetto di strumenti per il 5G. Introdurrebbe l'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: *quadro globale e orizzontale per affrontare i rischi di cibersicurezza per le catene di approvvigionamento delle TIC* – Questa opzione istituirebbe 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 delle TIC.

Dopo ampie analisi, il pacchetto strategico prescelto comprende: opzione A.2 - riforma del mandato dell'ENISA; e l'opzione C.2 - riforma del quadro europeo di certificazione della cibersicurezza, mediante la revisione della procedura e l'estensione dell'ambito di applicazione per agevolare le semplificazione della conformità normativa e opzione C.2 - Intervento mirato – ulteriore semplificazione della conformità al pertinente quadro normativo dell'Unione in materia di cibersicurezza) e l'opzione D.3 – Quadro globale e orizzontale per affrontare i rischi di cibersicurezza per le catene di approvvigionamento delle TIC.

Questa combinazione offre una risposta ben equilibrata alle sfide politiche individuate, migliorando in modo significativo l'efficacia, l'efficienza e la coerenza in tutta l'UE.

Impatti principali

Analisi costi-benefici: la transizione verso l'opzione prescelta proposta per il quadro normativo comporterà costi, sia per l'ENISA per lo svolgimento dei nuovi compiti (stimati fino a 161,3 milioni di EUR nell'arco di cinque anni) sia per le autorità pubbliche in tutta l'Unione per la vigilanza (stimati fino a 80 milioni di EUR nell'arco di cinque anni, tenendo conto dei pertinenti risparmi sui costi). Per quanto riguarda le imprese, durante il periodo di

transizione di tre anni l'eliminazione graduale di specifiche apparecchiature ad alto rischio potrebbe comportare costi annui compresi tra 3,4 e 4,3 miliardi di EUR per gli operatori di reti mobili, mentre gli investimenti in fornitori affidabili potrebbero contestualmente aumentare fino a 2 miliardi di EUR all'anno. Allo stesso tempo, la razionalizzazione e la riduzione degli obblighi di conformità dovrebbero generare risparmi sui costi fino a 14,6 miliardi di EUR per le imprese. Vantaggi significativi per i cittadini, le autorità pubbliche e le imprese deriverebbero inoltre dal miglioramento della postura di cibersicurezza complessiva dell'UE e della sua sovranità tecnologica e dalla promozione dell'innovazione e della competitività, che, secondo le attese, nel lungo periodo compenseranno in larga misura le spese iniziali.

Competitività: riducendo la frammentazione del mercato e armonizzando le normative, le opzioni prescelte rafforzano la parità di concorrenza in tutta l'UE, offrendo alle imprese percorsi più chiari verso la conformità e l'innovazione.

Controllo della coerenza climatica: la valutazione ha preso in considerazione il potenziale impatto ambientale di ciascuna opzione. Particolare attenzione è stata prestata all'efficienza energetica, alle emissioni legate ai viaggi e al consolidamento delle infrastrutture. Le opzioni prescelte A.2, B.2 e C.2 hanno un impatto ambientale limitato, mentre l'opzione D.3 tiene conto della neutralità ambientale, considerando il ciclo di vita del prodotto e i periodi di transizione per la sostituzione delle risorse chiave. Ciò è in linea con l'impegno dell'UE a favore della sostenibilità.

Digitale per default: la particolare attenzione riservata alla razionalizzazione dei processi digitali dimostra l'impegno dell'UE a favore di un approccio "digitale per default", che garantisca uno scambio di dati e un processo decisionale più rapidi e affidabili. Anche l'opzione D.3 potrebbe avere un forte impatto sulla digitalizzazione, in quanto comporterebbe la sostituzione di componenti provenienti da soggetti stabiliti in paesi terzi che destano preoccupazioni per la cibersicurezza o controllati da soggetti di tali paesi terzi.

Semplificazione e riduzione degli oneri: le opzioni prescelte contribuiscono alla semplificazione attraverso l'introduzione di chiarimenti sull'ambito di applicazione e misure volte a razionalizzare la conformità e la vigilanza, riducendo gli oneri amministrativi. Il principio "one in, one out" è considerato garantendo che i nuovi obblighi siano controbilanciati da riduzioni altrove.

Conclusioni

La presente valutazione d'impatto presenta una strategia globale per rafforzare la cibersicurezza dell'UE, affrontare le inefficienze normative e preparare il panorama digitale alle sfide future. Si raccomanda un approccio collaborativo e coeso, che basi le riforme politiche all'interno dei quadri esistenti e si adatti nel contempo alle nuove realtà tecnologiche. Attraverso queste misure l'UE mira a garantire un'economia digitale resiliente, competitiva e sostenibile.