REGOLAMENTI, DECISIONI E DIRETTIVE

REGOLAMENTO (UE, Euratom) 2023/2841 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 13 dicembre 2023

che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 298,

visto il trattato che istituisce la Comunità europea dell'energia atomica, in particolare l'articolo 106 bis,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

deliberando secondo la procedura legislativa ordinaria ([1]),

considerando quanto segue:

(1) Nell'era digitale, le tecnologie dell'informazione e della comunicazione sono fondamentali per un'amministrazione europea aperta, efficace ed indipendente. L'evoluzione della tecnologia e la maggiore complessità e interconnessione dei sistemi digitali amplificano i rischi per la cibersicurezza, rendendo i soggetti dell'Unione più vulnerabili alle minacce e agli incidenti informatici, il che rappresenta un pericolo per la loro continuità operativa e per la loro capacità di protezione dei dati. Se il maggior ricorso ai servizi cloud, l'uso generalizzato delle tecnologie dell'informazione e della comunicazione (TIC), l'elevato livello di digitalizzazione, il lavoro a distanza e l'evoluzione delle tecnologie e della connettività sono caratteristiche fondamentali di tutte le attività dei soggetti dell'Unione, la resilienza digitale non è ancora sufficientemente integrata.

(2) Il panorama delle minacce informatiche che pesano sui soggetti dell'Unione è in costante divenire. Gli autori delle minacce impiegano tattiche, tecniche e procedure in continua evoluzione, mentre i moventi più usuali per questi attacchi cambiano di poco: dal furto di importanti informazioni riservate al profitto finanziario, alla manipolazione dell'opinione pubblica o all'indebolimento delle infrastrutture digitali. Il ritmo di perpetrazione degli attacchi informatici da parte degli autori delle minacce continua a intensificarsi, con campagne sempre più sofisticate e automatizzate che prendono di mira le superfici di attacco esposte, che continuano ad ampliarsi, sfruttando rapidamente le vulnerabilità.

(3) Gli ambienti TIC dei soggetti dell'Unione sono interdipendenti, utilizzano flussi di dati integrati e sono caratterizzati da una stretta collaborazione fra i loro utenti. Tale interconnessione significa che qualsiasi perturbazione, anche se inizialmente limitata a un solo soggetto dell'Unione, può avere effetti a cascata più ampi, con potenziali ripercussioni negative di ampia portata e di lunga durata su altri soggetti dell'Unione. Inoltre, alcuni ambienti TIC dei soggetti dell'Unione sono connessi con gli ambienti TIC degli Stati membri, e un incidente in un soggetto dell'Unione può rappresentare un rischio per la cibersicurezza degli ambienti TIC degli Stati membri e viceversa. La condivisione di informazioni specifiche su un incidente può facilitare il rilevamento di minacce informatiche o incidenti analoghi che interessano gli Stati membri.

(4) I soggetti dell'Unione sono obiettivi interessanti, che si trovano ad affrontare sia autori di minacce molto esperti e dotati di risorse adeguate, sia altri tipi di minacce. Al tempo stesso, fra tali soggetti il livello e la maturità della ciberresilienza e la capacità di individuare e contrastare attività informatiche dolose variano in modo significativo. Ai fini del loro funzionamento, è quindi necessario che i soggetti dell'Unione raggiungano un livello comune elevato di cibersicurezza attraverso l'attuazione di misure di gestione dei rischi di cibersicurezza commisurate ai rischi per la cibersicurezza individuati, lo scambio di informazioni e la collaborazione.

([1]) Posizione del Parlamento europeo del 21 novembre 2023 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio dell'8 dicembre 2023.