Cybersecurity Act 2, per Ducci la sfida del phase out: sicurezza europea senza cancellare strumenti e investimenti

Descrizione

(Adnkronos) â?? Il nuovo Cybersecurity Act 2 introduce un meccanismo destinato a cambiare profondamente la gestione delle catene di approvvigionamento tecnologiche in Europa: sulla base di una valutazione del rischio a livello unionale, la Commissione potrÃ qualificare un Paese terzo come fonte di preoccupazione per la cybersicurezza e designare le sue imprese come fornitori ad alto rischio. Da questa decisione potranno discendere divieti, esclusioni e obblighi di sostituzione che riguarderanno reti, infrastrutture e prodotti.

Stefania Ducci, capo della divisione strategia e politiche di cybersicurezza in ambito Ue dellâ??Agenzia per la cybersicurezza nazionale, ha illustrato le implicazioni del dossier durante la conferenza â??Tecnologia, potere, regole: la nuova partita della sovranitÃ europeaâ?•, organizzata da Adnkronos e Open Gate Italia.

Lâ??Acn Ã¨ lâ??amministrazione capofila italiana nel negoziato sul Cybersecurity Act 2 e sta coinvolgendo le altre amministrazioni, il Dipartimento per gli Affari europei e il tessuto industriale. Lâ??Agenzia ha giÃ avviato consultazioni con operatori privati, soggetti sottoposti alla Nis 2 e imprese delle telecomunicazioni, direttamente interessate dal Titolo IV sulla sicurezza delle catene di approvvigionamento Ict.

Lâ??elemento di novitÃ Ã¨ il passaggio da un approccio prevalentemente tecnico a un meccanismo che comprende una valutazione geopolitica della provenienza. Una volta designato un Paese terzo, le sue aziende potranno essere considerate high-risk vendor e i soggetti sottoposti alla Nis 2 potrebbero non poter utilizzare componenti provenienti da quei fornitori, nÃ© nelle infrastrutture nÃ© nei prodotti realizzati. Lâ??impatto, ha sottolineato Ducci, sarebbe quindi esteso a una parte molto ampia del sistema produttivo.

Lâ??obiettivo europeo di ridurre dipendenze tecnologiche critiche Ã¨ condivisibile. Le catene Ict sono globali e interconnesse, e una vulnerabilitÃ presente in uno Stato membro puÃ² propagarsi allâ??intera Unione. Ma lâ??Europa non parte da zero. Diversi Paesi, e in particolare lâ??Italia, hanno giÃ costruito strumenti nazionali per gestire i rischi: Golden Power, perimetro di sicurezza nazionale cibernetica,

disciplina Nis e misure sulla protezione delle infrastrutture critiche.

Ducci ha richiamato anche la legge 90 del 2024, che introduce criteri premiali negli appalti pubblici per le aziende che utilizzano tecnologie provenienti da Stati membri dellâ??Ue, della Nato o da Paesi legati da accordi di collaborazione. Questo modello di white listing si differenzia dallâ??impostazione del Cybersecurity Act 2, che tende invece verso una blacklist europea dei fornitori ad alto rischio.

La vera sfida non Ã¨ scegliere tra livello europeo e nazionale, ma costruire un sistema multilivello. La valutazione comune del rischio deve convivere con gli strumenti giÃ adottati dagli Stati, rendendoli coerenti e interoperabili. Cancellare le esperienze nazionali produrrebbe incertezza e potrebbe indebolire capacitÃ che hanno giÃ dimostrato di funzionare.

Un secondo nodo riguarda tempi e proporzionalitÃ . Il phase out degli apparati non ha lo stesso impatto in tutti i Paesi e in tutte le reti. La disponibilitÃ di fornitori alternativi, le competenze professionali necessarie alla sostituzione e la diversa struttura degli operatori possono determinare costi e tempi molto differenti. Una domanda europea concentrata in un periodo breve potrebbe inoltre far aumentare i prezzi delle componenti e creare nuove strozzature.

Per Ducci, un termine di 36 mesi puÃ² non essere sufficiente. Le esperienze maturate in Paesi anglosassoni mostrano che operazioni analoghe sulle reti mobili hanno richiesto tempi almeno doppi. Una transizione troppo rapida rischierebbe non soltanto di pesare sui bilanci delle aziende, ma anche di produrre disservizi per cittadini e imprese.

Câ??Ã¨ poi un problema di certezza del diritto. Gli operatori hanno effettuato investimenti sulla base di autorizzazioni, prescrizioni e valutazioni adottate dalle autoritÃ nazionali. Le future misure europee dovranno quindi fondarsi su criteri oggettivi, trasparenti e verificabili, evitando di rendere retroattivamente insostenibili scelte compiute nel rispetto delle regole.

Il punto di equilibrio indicato dallâ??Acn Ã¨ una transizione graduale, proporzionata e basata sul rischio. La sicurezza delle catene di approvvigionamento richiede un quadro europeo, ma quel quadro deve riconoscere le capacitÃ nazionali, misurare la disponibilitÃ delle alternative e preservare la continuitÃ dei servizi. Solo cosÃ¬ il de-risking puÃ² rafforzare la resilienza senza generare nuove vulnerabilitÃ economiche e operative.

â??

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Luglio 23, 2026
Autore

redazione