Cybersecurity, alla Pa forniture solo se con standard avanzati

Contratti pubblici

Con lo schema di Ddl gare con elementi essenziali anti hacker

Imprese del settore vincolate e c'è il rischio di essere esclusi dall'appalto

Ivan Cimmarusti
ROMA

ADOBESTOCK

La stretta. Per partecipare alle gare di fornitura per la Pa le aziende dovranno garantire profili di cybersecurity o saranno escluse

Nell'approvvigionamento di beni e servizi informatici in un «contesto connesso alla tutela degli interessi nazionali strategici», la Pubblica amministrazione dovrà tenere presente «gli elementi essenziali di cybersicurezza». Tradotto: le imprese del settore per partecipare alle gare di fornitura dovranno garantire questi profili di sicurezza, viceversa saranno escluse.

L'annunciata stretta entra nel Ddl Cybersicurezza, varato ieri dal Consiglio dei ministri, che ora viaggia spedito verso il passaggio parlamentare. Difficile una marcia indietro: i servizi di informazione e sicurezza registrano una costante emergenza legata agli attacchi hacker, cui vanno aggiunte le analisi del servizio di Polizia Postale e delle Comunicazioni, che nel bilancio 2023 hanno rilevato 11.930 attacchi soprattutto verso infrastrutture critiche e istituzioni. Aspetti sotto la lente dell'Agenzia per la cybersicurezza nazionale - sotto la direzione di Bruno Frattasi e la vicedirezione di Nunzia Ciardi - all'interno della quale opera un apposito Nucleo cui ora faranno parte anche la Direzione nazionale antimafia e la Banca d'Italia, segno che gli attacchi hacker possono celare la mano mafiosa, con gravi riflessi in ambito riciclaggio. Ma andiamo con ordine.

Lo schema di Ddl prevede che «con decreto del presidente del Consiglio dei ministri, da adottarsi entro 120 giorni dalla data di entrata in vigore» della legge, «su proposta dell'Agenzia per la cybersicurezza nazionale, previo parere del Comitato interministeriale per la cybersicurezza» siano individuati «gli elementi essenziali di cybersicurezza» che dovranno essere considerati dalle Pa nell'approvvigionamento delle infrastrutture informatiche.

Secondo il Ddl, per elementi essenziali di cybersicurezza «si intende l'insieme di standard e regole tecniche la cui conformità da parte di beni e servizi informatici da acquisire garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare in misura corrispondente alle esigenze di tutela» cyber.

Destinatari della misura sono: tutte le amministrazioni dello Stato (articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82), compresi gli istituti e le scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane e loro consorzi e associazioni. Ci sono poi le università, gli istituti autonomi case popolari, le Camere di commercio e associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale. Tra i destinatari ci sono anche i soggetti privati (previsti dall'articolo 1, comma 2-bis Dl 21 settembre 2019, n. 105), in relazione a determinati settori strategici.

> **I principi di sicurezza informatica saranno individuati entro 120 giorni dall'entrata in vigore della norma**

Ma veniamo all'impatto che la misura può avere sulle imprese. L'ente pubblico quando rileva che l'offerta non tenga in considerazione gli elementi essenziali di cybersicurezza individuati dal decreto, può applicare l'articolo 107, comma 2, e 108, comma 10 del decreto legislativo 36/2023: «La stazione appaltante può decidere di non aggiudicare l'appalto all'offerente che ha presentato l'offerta economicamente più vantaggiosa se ha accertato che l'offerta non soddisfa gli obblighi».