PA ALLA PROVA DELLA SICUREZZA INFORMATICA

di **Brunella Bruno**

Dal 16 ottobre è in vigore il Dlgs 138/2024, di recepimento della direttiva NIS2 – (UE) 2022/2555, volta a rafforzare la sicurezza delle reti e dei sistemi informativi, specie nei settori essenziali e critici che riguardano le pubbliche amministrazioni.

Il decreto interviene a soli tre mesi di distanza dall'entrata in vigore della legge 90/2024, complementare alla direttiva NIS2 e con la quale sono stati imposti ulteriori obblighi di sicurezza gravanti sulla Pa, nonché introdotte modifiche al Codice penale, con la previsione di nuove fattispecie di reato e inasprimento delle pene per i crimini informatici. L'attualità della questione è nota, come dimostrato dai recenti episodi di violazione di banche dati anche di importanti amministrazioni pubbliche. Oltre all'obbligo di segnalazione tempestiva all'Agenzia per la cybersicurezza nazionale di incidenti informatici, si prevedono strutture interne dedicate e la nomina di un referente per la cybersicurezza.

L'adeguamento agli sviluppi normativi impone una trasformazione culturale e organizzativa nella Pa. La predisposizione di un programma di cybersecurity non riveste più caratteristiche discrezionali e, in considerazione della frammentazione normativa in materia, la compliance costituisce un fattore complesso da gestire ma essenziale per evitare anche l'esposizione a responsabilità, acuita dalla circostanza che l'evoluzione di tecnologie e rischi fa sì che le conseguenze di incidenti e attacchi su terze parti possono dispiegarsi pure a distanza di tempo. Ciò implica un'attenta valutazione della conformità anche agli standard internazionali di sicurezza e protezione dei dati, oltre che dei rischi, competendo al referente per la cybersecurity la relativa gestione, incluso il monitoraggio dei fornitori di servizi digitali e tecnologici, su tutta la supply chain.

La cybersecurity esige un approccio operativo e sostanziale, che deve tradursi nell'attuazione di numerose misure: formazione degli utenti; approvvigionamento di prodotti e servizi; regolazione dei processi; controllo della sicurezza applicativa; monitoraggio degli accessi ai sistemi sulla base di procedure garantite, incentrate su indicatori di anomalia calibrati sullo specifico settore di interesse. Si tratta di interventi difficilmente esigibili a invarianza finanziaria, come purtroppo impone il Dlgs 138/2024.

Centralità riveste, inoltre, l'autenticità, intesa quale certa identificazione di chi interagisce nei sistemi, che condiziona la fiducia nelle interazioni digitali e la stessa integrità dei processi, specie nell'attuale fase di impiego di tecnologie sempre più sofisticate come l'IA. La trasformazione digitale della Pa sta determinando un irreversibile riassetto organizzativo e sulle regole di esercizio dei poteri pubblici. Le modalità di controllo e l'imputazione univoca dell'accesso ai servizi dell'amministrazione, con livelli di sicurezza parametrati agli scenari di utilizzo, costituiscono precondizioni per uno sviluppo sicuro e garantito, emergendo, quindi, anche la saldatura della direttiva NIS2 con il regolamento Eidas 2.0 (2024/1183) e la relativa disciplina di attuazione. L'introduzione dell'European digital identity wallet e, a livello nazionale, il sistema IT Wallet, mirano a favorire la fruizione di servizi pubblici e privati da parte dei cittadini europei, la cui accessibilità, sicura e affidabile, richiede impegni convergenti; da un lato quello degli utenti nella direzione che non vi può essere alcuno "scambio" tra sicurezza ed efficienza; dall'altro quello istituzionale per una più esaustiva considerazione delle esigenze concrete degli utenti, specie di quelli che svolgono attività qualificate. Il riferimento è, al riguardo, a una riconsiderazione dello spid a uso professionale, che necessità di essere meglio plasmato sulle specifiche attività.

La particolare delicatezza e rilevanza di determinati settori, tra i quali quello dei contratti pubblici, dovrebbe, peraltro, indurre a valutare l'opportunità dell'attribuzione dell'attività di certificazione delle piattaforme e dei sistemi operativi a un organismo pubblico qualificato, sul modello del Centro di valutazione e certificazione nazionale, con vantaggi sul piano della semplificazione delle attività, maggiore sostenibilità degli oneri e più piene garanzie sotto molteplici profili.

—Continua a pagina 36