MF MILANO FINANZA

diffusione:98970
tiratura:162805

COMMENTI & ANALISI

La strategia cloud nazionale deve essere basata sulla concorrenza e sull'Europa

DI STEFANO DA EMPOLI*

Negli ultimi anni il cloud computing ha rapidamente assunto un particolare valore strategico come piattaforma abilitante per la trasformazione digitale, dettando il passaggio da un sistema in cui ogni individuo o organizzazione dispone di propri hardware e software ad un nuovo contesto più fluido in cui gli utenti possono fruire dei servizi e delle infrastrutture It in base alle proprie necessità, a richiesta. In questo modo il processo di riforma potrà così contare sulle migliori tecnologie, a costi estremamente competitivi.

Il Piano Nazionale di Ripresa e Resilienza (Pnrr) riconosce una piena centralità al cloud, prevedendo di riservare almeno il 10% delle risorse del programma Transizione 4.0 all'acquisto di beni intangibili digitali da parte delle imprese e dedicando un miliardo di euro dei 6,14 destinati alla digitalizzazione della pubblica amministrazione alla migrazione verso il cloud delle amministrazioni pubbliche. Che dovranno seguire un approccio «cloud-first» che nei prossimi anni darà loro la possibilità di scegliere «se migrare verso una nuova infrastruttura cloud nazionale all'avanguardia (Polo Strategico Nazionale-Psn) o verso un cloud pubblico sicuro, a seconda della sensibilità dei dati e dei servizi coinvolti».

Laddove il pubblico, nella terminologia cloud, non si riferisce alla proprietà bensì alla condivisione di una pluralità di clienti delle stesse infrastrutture, naturalmente in condizioni di privacy e sicurezza. Questa forma di cloud, che potremmo dunque definire di mercato, ha due vantaggi essenziali: è il solo che può sfruttare al massimo la flessibilità e scalabilità proprie del cloud e ha la capacità di offrire servizi on top ad alto valore aggiunto (per esempio data analytics, machine learning). Solo che, spesso erroneamente, si riconosce al cloud pubblico un livello di sicurezza minore rispetto a quello privato, in base al quale ogni organizzazione ha un proprio data center esclusivo.

La verità è che la stragrande maggioranza di questi data center, oltre a rappresentare uno spreco di risorse, presenta livelli di sicurezza decisamente peggiori rispetto agli standard medi del cloud pubblico. Una prospettiva riconosciuta nello stesso Pnrr, che rileva come il 95% dei circa 11mila data center utilizzati dagli enti pubblici italiani presenti oggi carenze nei requisiti minimi di sicurezza, affidabilità, capacità elaborativa ed efficienza.

Ecco perché nella costruzione di una strategia cloud nazionale occorre un approccio equilibrato, basato sui fatti.

In questo senso il Pnrr rappresenta un primo step, che deve tuttavia essere messo a terra con indicazioni precise e stringenti, soprattutto rispetto alle scelte delle amministrazioni pubbliche.

Sono assolutamente da evitare esperienze fallimentari come quella del progetto Andromède francese di cloud «sovrano», che avrebbe dovuto essere realizzato attraverso un partenariato pubblico-privato con lo Stato in qualità di azionista di maggioranza. Tuttavia, il progetto iniziale è naufragato, portando all'uscita dei soggetti pubblici e all'interruzione dei servizi inizialmente previsti.

Iniziative fondate su un approccio più pragmatico e aperto alla concorrenza si sono rivelate più efficaci. Come quella britannica, che ha puntato su una pluralità di accordi con i cloud provider privati e su una Data classification strategy, basata su tre livelli di sicurezza, tesi a distinguere informazioni classificate come «secret» e «top secret» (in tutto non più del 5% del totale) dal resto, che può rimanere nel cloud pubblico.

Sempre guardando al di là dei nostri confini, di recente è stato promosso a livello europeo il progetto Gaia-X, che implica la creazione di un ecosistema basato su regole e valori comuni, al quale possono partecipare tutti gli attori con le carte in regola per farne parte.

La dimensione europea è quella giusta nella quale assicurare insieme concorrenza e sicurezza nella fornitura dei servizi cloud. L'apertura del mercato a tutti i cloud service provider nazionali e internazionali che possano assicurare standard adeguati di sicurezza favorisce da un lato maggiori investimenti, italiani ed esteri, in innovazione, infrastrutture e tecnologie sul territorio nazionale e, allo stesso tempo, incoraggia l'interoperabilità dei servizi e la portabilità di dati e applicazioni, secondo i principi guida delineati nella Strategia europea dei dati, pubblicata nel 2020.

La sicurezza va perseguita attraverso una classificazione rigorosa di dati e asset strategici per valutare quali sono quelli che necessitano di un particolare livello di protezione, con criteri che garantiscano il migliore trade-off tra sicurezza e competitività del mercato.

Solo tenendo alla larga tentazioni protezionistiche e autarchiche, si raggiunge una sovranità digitale effettiva, che deriva dalla capacità di cogliere appieno le sfide portate dalle nuove tecnologie, massimizzandone i benefici e controllandone i rischi. (riproduzione riservata)