L'isolamento porta in un *vicolo cieco digitale*

22.11.2026

A colpo d'occhio

- L'UE intende escludere in larga misura i fornitori di servizi cloud provenienti da Paesi terzi dagli appalti pubblici sensibili, compresi quelli svizzeri.
- Questa è la conseguenza di un dibattito che si sta svolgendo con grande intensità anche in Svizzera.
- Lo sguardo rivolto a Bruxelles mostra quali possono essere le conseguenze di un isolamento digitale sistematico.

Cosa prevede il CADA

Il 3 giugno 2026 la Commissione europea ha presentato il suo «Tech Sovereignty Package». Si compone del Chips Act 2.0, di una strategia open source, di una tabella di marcia per la digitalizzazione nel settore energetico e, come elemento centrale, del Cloud and AI Development Act (CADA). Oltre a velocizzare le autorizzazioni per i centri di calcolo, il CADA introduce quattro livelli di sovranità per i servizi cloud. Questi livelli determinano quali fornitori sono ammessi per compiti pubblici rilevanti per la sicurezza e per gli appalti. Tra i requisiti ci sono l'elaborazione dei dati all'interno dell'UE e la protezione dall'accesso da parte di paesi terzi. I fornitori esteri possono essere presi in considerazione al massimo al livello 3, e solo se il loro mercato nazionale è aperto e garantisce all'UE un accesso equivalente. Nelle gare d'appalto, inoltre, dovrebbe contare il «valore aggiunto UE», ovvero software e hardware sviluppati nell'UE. Per la Svizzera questo significa che i centri di calcolo sul nostro territorio non soddisfano nemmeno i requisiti del livello base, perché l'archiviazione e l'elaborazione dei dati devono avvenire nell'Unione. Per ora è solo una proposta, ma la direzione è chiara.

L'origine non è un criterio di sicurezza

Bruxelles parla di «sovranità digitale». Ma sovranità non significa affatto sicurezza. Ciò che conta è cosa offre un fornitore e quanto bene protegge i dati, non da dove viene. Il CADA, invece, si basa sull'origine e considera un rischio persino la Svizzera, un paese fondato sullo Stato di diritto e strettamente legato all'UE. Quanto poco la provenienza dica sulla sicurezza lo dimostra la Danimarca: alcuni hacker hanno sfruttato l'accesso legittimo di una piccola azienda informatica locale al registro anagrafico e hanno sottratto i dati di 8,8 milioni di persone, più del numero totale di abitanti del paese. A quanto pare, è bastata la password «123456». Chi definisce l'origine come un criterio di sicurezza, quindi, fa soprattutto una cosa: politica di accesso al mercato con l'etichetta della sovranità.

I mercati aperti sono fondamentali per la Svizzera

La Svizzera conosce questa logica dal lato opposto. Gli Stati Uniti giustificano espressamente i loro dazi farmaceutici con l'obiettivo di potenziare la produzione interna e ridurre le dipendenze. L'industria farmaceutica svizzera, che destina quasi il 30 per cento delle sue esportazioni agli Stati Uniti, e la Confederazione vedono giustamente in questo un peso per la Svizzera come piazza economica. A nessuno verrebbe in mente di celebrarlo come un contributo alla sicurezza dell'approvvigionamento. Lo stesso vale, in senso inverso, per l'oro, dove è il mondo a dipendere da noi: secondo i dati del settore, circa due terzi dell'oro raffinato a livello mondiale passa attraverso le raffinerie svizzere. Ne traiamo vantaggio solo perché i mercati sono aperti. Un mondo in cui ogni paese insistesse sull'origine di ogni bene sarebbe un male per la Svizzera.

Moderazione anche in casa nostra

Anche nel nostro Paese si discute di sovranità digitale. In Parlamento si parla di un'infrastruttura sovrana propria, di programmi di stimolo con fondi pubblici e di dare più peso ai fornitori nazionali. Le richieste sono comprensibili. Il CADA, però, mostra dove stanno i limiti: se altri applicassero la stessa logica in modo coerente, il settore IT nazionale si troverebbe davanti a porte chiuse. I requisiti di provenienza dovrebbero quindi essere applicati con moderazione anche a livello nazionale.

Il Consiglio federale dimostra che si può fare anche diversamente. Il 20 ottobre ha indetto una gara d'appalto per lo Swiss Government Cloud, con un volume fino a 7 miliardi di franchi in 14 anni. Invece di escludere in blocco i fornitori stranieri, punta su una strategia multi-cloud a tre livelli, suddivisa in cinque lotti: un public cloud globale per i dati meno sensibili, un public cloud con archiviazione dei dati in Svizzera e un private cloud nei centri di calcolo della Confederazione. Ogni fornitore può aggiudicarsi un solo lotto; dopo sette anni il mercato verrà riaperto. Si tratta di una soluzione complessa dal punto di vista dell'architettura, che comporta un certo onere amministrativo, ad esempio a causa dei numerosi contratti e accordi sul livello di servizio. Ma è la strada più intelligente da seguire. Permette di gestire le dipendenze, invece di nasconderle dietro divieti di provenienza.

Cosa fare ora

Il Consiglio federale dovrebbe impegnarsi a Bruxelles affinché i fornitori svizzeri siano riconosciuti ai sensi del CADA. La sua carta vincente è proprio la gara d'appalto per lo Swiss Government Cloud: chi chiede apertura all'UE deve averla dimostrata in prima persona. I mercati aperti sono l'assicurazione sulla vita per un paese esportatore. Valgono però in entrambe le direzioni.

Questo articolo è stato pubblicato per la prima volta il 22 novembre 2026 su netzwoche.ch

© economiesuisse | www.economiesuisse.ch