economiesuisse

Cibersicurezza: la cooperazione batte l'imposizione statale

L'imposizione da parte dello Stato e l'eccessiva regolamentazione sono solitamente controproducenti, soprattutto in un settore come quello della cibersicurezza, in cui tutte le parti interessate perseguono lo stesso obiettivo. Sono necessarie cooperazione e soluzioni pratiche. Il tema è attuale, come la politica federale ha recentemente dimostrato tramite l'inasprimento della legge sulla sicurezza delle informazioni (LSIn). Anche l'economia è favorevole a una forte attenzione alla cibersicurezza.

Quando si parla di cibersicurezza, tutti gli attori della politica, dell'economia e della società condividono un interesse comune: la protezione dei dati sensibili e delle infrastrutture critiche. Nonostante questa armoniosa posizione di partenza, la politica federale si concentra sempre più sulla regolamentazione statale e sulle misure coercitive, come il recente inasprimento della legge sulla sicurezza delle informazioni (LSIn). La fiducia nelle imprese svizzere sembra essere bassa. Tuttavia, l'introduzione di un "programma obbligatorio" imposto dallo Stato non è una buona idea in questo settore specifico e non è né efficace né efficiente. La strada per una maggiore sicurezza non passa attraverso una maggiore regolamentazione e non deve essere intrapresa "contro" le imprese. Anche ulteriori misure proposte, come quelle attualmente in discussione nell'ambito della mozione 24.3810, sono più dannose che utili in questo contesto.

«Invece di affidarsi alle imposizioni, i politici dovrebbero basarsi sulla cooperazione.»

La revisione dell'LSIn e ora anche la bozza della prevista ordinanza sulla cibersicurezza hanno dimostrato che in questo settore altamente sensibile lo Stato cade costantemente in una concezione del proprio ruolo che fa più male che bene. Da un lato, utilizza misure obbligatorie per assumersi una responsabilità che non è in grado di gestire, mentre dall'altro crea ostacoli inutili per le imprese che stanno già investendo attivamente nella loro sicurezza. In terzo luogo, inibisce una sana cultura dell'errore. Invece di affidarsi all'imposizione, i responsabili politici dovrebbero perseguire un approccio cooperativo in cui tutte le parti interessate possano contribuire con le loro competenze e risorse.

Non avrebbe molto senso che la polizia controllasse la resistenza dei lucchetti delle biciclette (a spese dei proprietari) sulle rastrelliere e penalizzasse coloro che utilizzano lucchetti presumibilmente troppo deboli. L'obiettivo dovrebbe invece

essere quello di comunicare chiaramente quali sono i lucchetti che offrono vantaggi in termini di sicurezza. La responsabilità rimane del proprietario, che decide autonomamente quali misure sono più opportune per lui. Lo stesso vale per la cibersicurezza: l'imposizione e le sanzioni da sole non servono. È più importante che le imprese sappiano quali misure sono realmente efficaci per proteggere i loro sistemi.

L'obiettivo dovrebbe essere quello di creare condizioni quadro sicure basate sulla fiducia, sulla cooperazione e su misure praticabili. Dopotutto, la cibersicurezza non può essere raggiunta con una mentalità da "casco totale", in cui ogni lacuna deve essere colmata dal controllo del governo. È invece necessario un sistema di gestione di chiavi equilibrato, proprio come nella vita di tutti i giorni, quando mettiamo in sicurezza le nostre case senza sbarrarle completamente. Questo è l'unico modo per ottenere una strategia di sicurezza efficiente e sostenibile.

I progressi tecnologici nel campo della cibersicurezza sono rapidi e nuove soluzioni stanno emergendo grazie alla concorrenza e all'innovazione creativa. Un eccesso di regolamentazione statale potrebbe ostacolare questo sviluppo e limitare la capacità di adattamento del mercato. La cibersicurezza non è un fine in sé, né un problema che può essere risolto con un numero sempre maggiore di paragrafi. Può essere risolta solo con praticità, cooperazione e pragmatismo.