

Li sovranità digitale: pilastro strategico per l'Indipendenza e l'innovazione di un Paese

Rrlazione tenuta in occasione dell'incontro annuale della Segreteria di Stato per gli Affari Esteri con il Corpo Diplomatico e Consolare sammarinese, svoltosi presso l'Aula Magna "Fausta Morganti" dell'Università degli Studi della Repubblica di San Marino.

di Nicola Barone



Nicola Barone

1. Introduzione: I dati come asset e il cloud come "raffineria"

Nel paradigma economico del Cloud e dell'Intelligenza Artificiale, la sovranità digitale non è un'opzione tecnica, ma un **imperativo di sicurezza nazionale e sopravvivenza economica**. Governare l'infrastruttura significa proteggere

l'autonomia decisionale di un intero Paese. Come sottolineato dal Presidente della Repubblica Italiana Sergio Mattarella, lo strapotere delle corporazioni globali rischia di configurare nuove "Compagnie delle Indie" che esercitano poteri estranei al controllo degli Stati e degli organismi internazionali. In questo scenario, i dati rappresentano il "nuovo petrolio", ma il dato grezzo è privo di valore intrinseco: la sua utilità risiede nella capacità di raccolta, analisi e protezione.

Le infrastrutture Cloud agiscono oggi come le **raffinerie digitali del XXI secolo**. Senza una "raffinazione" sicura e locale, il patrimonio informativo nazionale viene svenduto o esposto a rischi inaccettabili. La dipendenza da operatori soggetti a giurisdizioni extra-territoriali crea vulnerabilità strutturali. Il caso della **polizia scozzese**, a cui Microsoft ha recentemente negato dettagli sui flussi di dati invocando la "riservatezza commerciale", dimostra plasticamente come il controllo dei flussi informativi sia oggi una terra di confine dove il diritto nazionale rischia di soccombere davanti a normative straniere come il Cloud Act. Per mitigare tale vulnerabilità strategica, è necessario declinare la sovranità su tre livelli di controllo chiari e progressivi.

2. L'architettura della sovranità: I tre livelli fondamentali

La sovranità digitale deve essere intesa come una capacità modulare, non binaria, che si adatta al profilo di rischio dell'organizzazione. Come evidenziato nel **Rapporto Draghi sulla competitività**, l'Europa non può permettersi di abbandonare il controllo in ambiti cruciali come la sicurezza e la crittografia.

2.1 Sovranità dei dati (controllo giuridico)

Definisce la capacità di esercitare il controllo decisionale sulle informazioni, garantendo che la giurisdizione del dato coincida con il territorio in cui esso risiede. La localizzazione logica e geografica è la condizione *sine qua non* per la conformità a norme locali sulla riservatezza dei dati e per la protezione dalle leggi extraterritoriali che impongono l'accesso ai dati senza il consenso del titolare.

Senza sovranità giuridica, i segreti industriali e i brevetti di un'azienda sono legalmente "espropriabili" da autorità straniere, minando la fiducia degli investitori e la proprietà intellettuale.

Vale altresì la pena evidenziare come alcune già citate norme extraterritoriali rappresentino ad oggi un'area dove il diritto internazionale non ha ancora trovato una soluzione valida ed è quindi nel contesto tecnologico che invece si possono trovare delle contromisure. L'uso di chiavi crittografiche gestite da operatori nazionali fornisce ad esempio uno strumento per evitare l'accesso ai dati a soggetti non autorizzati.

2.2 Sovranità operativa (resilienza)

Riguarda la continuità dei servizi essenziali in scenari di crisi geopolitica. Gestire backup e disaster recovery sotto controllo locale garantisce l'autonomia di risposta. Il rischio è il cosiddetto "**Scenario Starlink**": come dichiarato da Elon Musk, la capacità di spegnere un'infrastruttura critica con un click può determinare il collasso di intere linee di difesa o servizi pubblici.

La resilienza operativa, quindi, trasforma la continuità del business e dei servizi digitali pubblici da una dipendenza esterna a una capacità autonoma, essenziale per la stabilità delle infrastrutture critiche (energia, trasporti, sanità).

2.3 Sovranità tecnologica (autonomia)

Mira a ridurre il rischio di *vendor lock-in*, ovvero una dipendenza forte da uno o più soggetti tecnologici, ed a garantire visibilità totale sulla supply chain. Utilizzare standard aperti e mantenere il controllo delle competenze ICT permette di non subire passivamente le roadmap tecnologiche dei provider globali.

L'autonomia tecnologica evita la trappola del "same services, same rules", permettendo alle imprese di innovare secondo le proprie specificità industriali e non secondo modelli imposti da oligopoli esteri.

3. Un approccio pragmatico alla sovranità

Fermo restando quanto sopra, sarebbe errato associare la Sovranità digitale ad una forma di isolazionismo tecnologico. La governance della sovranità deve essere adattiva, integrando l'innovazione globale degli hyperscaler con la protezione, la gestione e l'autonomia locale. Non è una questione di autarchia, ma di **autonomia strategica**.

Un punto di partenza fondamentale è dotarsi di un modello di classificazione dei dati, che tenga conto della loro rilevanza e del danno derivante da una loro compromissione.

Usando ad esempio la classificazione usata in Italia, avremmo

1. **Dati Ordinari:** possono essere mantenuti in cloud, con delle garanzie medie
2. **Dati Critici:** sono dati che richiedono elevati standard di sicurezza e sovranità, ottenibili su cloud pubblici solo a patto di complesse componenti aggiuntive

3. Dati Strategici: la conservazione di questi dati può avvenire solo su infrastrutture a piena giurisdizione nazionale (es. per l'Italia, il Polo Strategico Nazionale).

Sulla base di questa classificazione, si dovranno poi operare scelte che bilancino un uso di tecnologia avanzata come quella degli hyperscaler, con soluzioni di provider locali o frutto di partenariati pubblico-privati, che offrono maggiori garanzie di sovranità. Proprio grazie al coinvolgimento del settore pubblico, infatti, sarà possibile costruire un ecosistema propizio per investimenti privati che vadano nella direzione di colmare l'attuale divario tecnologico che c'è, nell'ambito digitale, tra Europa e Stati Uniti e Cina. A tal fine vale la pena ricordare come la sovranità digitale sia anche uno degli obiettivi fondamentali del Digital Compass 2030, un piano di interventi per realizzare la trasformazione digitale dei Paesi UE, presentato dalla Commissione Europea il 9 marzo 2021 e che si sviluppa lungo il "decennio digitale europeo", dal 2021 al 2030.

Conclusione: la sovranità come garanzia di indipendenza strategica

La sovranità digitale è la sfida del nostro tempo. Coniugare innovazione tecnologica e sicurezza strategica e sociale sono un tema complesso che non va affrontato con slogan o con semplificazioni o superficialità. Non rappresenta un isolamento autarchico, ma una condizione di libertà economica che abilita l'innovazione sicura e permette di negoziare accordi tecnologici da una posizione di forza, non di sudditanza.

Investire in autonomia digitale significa sottoscrivere una **polizza di sicurezza geopolitica**. In un mondo guidato dai dati ed in cui gli equilibri e le regole internazionali si stanno riscrivendo, troppo spesso non attraverso la diplomazia ma tramite forzature ed imposizioni, l'inerzia non è un costo accettabile: è una minaccia alla continuità stessa della società e delle singole nazioni. Il momento di agire è adesso.

San Marino, 2 settembre 2026