

<https://thecradle.co/>
18 febbraio 2026

Il Libano, la nuvola e i limiti della sovranità

Jamal Meselmani

Allineandosi con Oracle, il Libano colloca il suo futuro digitale all'interno di un ecosistema tecnologico statunitense strettamente legato a quello israeliano. potere di sicurezza.

L'8 dicembre 2025 il Libano presentò quella che sembrò una svolta tecnica.

L'azienda americana Oracle e il ministro di Stato libanese per la tecnologia e l'intelligenza artificiale, Kamal Shehadeh, hanno firmato un memorandum d'intesa strategico (MoU) impegnandosi a **formare 50.000** partecipanti del settore pubblico e privato nei prossimi cinque anni nei settori del cloud computing, dell'intelligenza artificiale (IA) e dell'apprendimento automatico.

I funzionari hanno descritto l'accordo come una "concessione gratuita", parte di un programma nazionale progettato per preparare il Libano all'era dell'intelligenza artificiale. In un Paese che sta affrontando il collasso economico e il declino istituzionale, il governo ha descritto l'accordo come un passo verso il rinnovamento digitale.

Tuttavia, nell'Asia occidentale, dove le guerre si sviluppano sempre più attraverso l'integrazione dei dati e il predominio delle comunicazioni, l'architettura cloud funziona come il sistema operativo dello Stato. **Controllo** Su tale architettura si plasmano la continuità fiscale, la resistenza amministrativa e la resilienza in termini di sicurezza. L'allineamento del Libano, quindi, si estende ben oltre la formazione della forza lavoro e tocca il terreno del controllo sovrano.

La formazione come allineamento strutturale

Il ministro Shehadeh ha **insistito** che l'accordo "non include lo scambio di dati o l'accesso alle informazioni del settore pubblico" ed è strettamente limitato alla formazione di 50.000 dipendenti libanesi membri.

Tali garanzie affrontano preoccupazioni immediate, ma lasciano intatte le implicazioni architettoniche derivanti dalla calibrazione di un'intera generazione di dipendenti pubblici e ingegneri su un unico ecosistema proprietario.

Il cloud computing definisce l'ambiente in cui vengono sviluppati e gestiti sistemi fiscali, registri di identità, piattaforme doganali, database sanitari, meccanismi di compensazione finanziaria e infrastrutture di sicurezza. La formazione di decine di migliaia di persone all'interno del framework proprietario di Oracle standardizza la logica istituzionale e i futuri percorsi di approvvigionamento.

I programmi di formazione di Oracle si concentrano quasi esclusivamente sul proprio **software proprietario** e sistemi aziendali. Lo sviluppo delle capacità secondo gli standard di un fornitore influenza inevitabilmente i requisiti di compatibilità, la progettazione dei sistemi e i quadri di governance digitale tra ministeri e agenzie.

La dipendenza cresce silenziosamente. Non appena i sistemi di stato vengono scritti all'interno di un'unica architettura, il prezzo da pagare per abbandonarla aumenta. I contratti di manutenzione, gli aggiornamenti software e l'integrazione della sicurezza informatica vincolano le istituzioni allo stesso quadro normativo nel tempo.

Per uno Stato alle prese con il collasso fiscale, l'ingarbugliamento architettonico comporta implicazioni strategiche che vanno ben oltre l'attuazione immediata.

Giurisdizione e leva finanziaria

Nell'era digitale la sovranità è inscindibile dalla giurisdizione.

Oracle opera secondo la legge statunitense. Il chiarimento legale del 2018

Legge sull'uso dei dati all'estero – **CLOUD Act** – garantisce alle autorità americane la possibilità di obbligare le aziende con sede negli Stati Uniti a fornire dati secondo quadri giuridici definiti, indipendentemente da dove tali dati siano fisicamente archiviati. La nazionalità aziendale, in questo senso, conferisce un'autorità giuridica che trascende la geografia.

I funzionari libanesi sottolineano che nessun dato pubblico verrà scambiato ai sensi del Memorandum d'intesa. La questione più ampia riguarda il controllo dell'ambiente operativo in cui i dati vengono creati, crittografati, elaborati, aggiornati e protetti.

Affidarsi a un'infrastruttura di origine americana comporta anche l'esposizione a decisioni normative statunitensi, sospensioni dei servizi o controlli sugli aggiornamenti software durante periodi di tensione politica.

L'integrazione tecnologica genera una leva finanziaria che può rivelarsi determinante durante una crisi.

Il CLOUD Act opera all'interno di una rete di condivisione di informazioni più ampia nota come **Five Eyes** – collegando Stati Uniti, Gran Bretagna, Canada, Australia e Nuova Zelanda in un framework di intelligence dei segnali altamente integrato. Nell'era del cloud, l'integrazione dell'intelligence si estende oltre le comunicazioni intercettate, fino all'architettura attraverso cui vengono gestiti i flussi di dati.

Il Libano entra in questo ecosistema senza una moderna legge sulla governance dei dati, senza un regime nazionale di classificazione delle informazioni sensibili, senza una gestione sovrana delle chiavi di crittografia e senza una strategia cloud multi-vendor.

L'allineamento architettonico in assenza di garanzie istituzionali aumenta l'asimmetria strutturale.

La supremazia dei dati sul fronte settentrionale

L'equilibrio di potere regionale chiarisce la posta in gioco, poiché la dottrina militare israeliana integra i sistemi di dati direttamente nella pianificazione operativa. Il concetto di Network-Centric Targeting fonde metadati di comunicazione, movimenti di popolazione e...

modelli, immagini di sorveglianza e intelligence open source (OSINT) in **cicli di targeting in tempo reale**.

Le finestre decisionali si restringono e la precisione degli attacchi si affina, mentre **gli ambienti civili** vengono trasformati in strutture di dati mappate che possono essere lette, elaborate e utilizzate quasi istantaneamente.

Tale capacità dipende da un'infrastruttura di calcolo su scala cloud in grado di elaborare enormi flussi di dati in pochi secondi.

Il progetto Nimbus di Israele – il trasferimento di importanti segmenti dell'infrastruttura digitale governativa in ambienti cloud gestiti da aziende tecnologiche statunitensi – rifletteva una dottrina di continuità sotto attacco, garantendo la resilienza operativa anche quando l'infrastruttura fisica veniva attaccata.

Il Libano ha subito le conseguenze dello squilibrio dell'intelligence. L'accesso israeliano alle telecomunicazioni libanesi ha **consentito** Avvisi localizzati, monitoraggio in tempo reale e omicidi mirati durante le recenti escalation. La vulnerabilità digitale si è tradotta in uno svantaggio strategico, rafforzando l'asimmetria che caratterizza il fronte settentrionale.

Questa realtà non richiede presupposti teorici per essere compresa. In un centro di telecomunicazioni ai margini di un'area di confine meridionale, dove le chiamate provenienti da interi villaggi passano attraverso file di rack metallici illuminati da deboli indicatori verdi, un tecnico notò una volta che il traffico dati si comportava in modo insolito durante un periodo di tensione. Non c'era un carico di rete eccezionale né interruzioni di corrente, eppure alcune rotte perdevano brevemente stabilità per alcuni secondi prima di tornare alla normalità. Per gli utenti, nulla sembrava anomalo; le chiamate continuavano e Internet rimaneva funzionante. Ma per coloro che leggono le reti come i pianificatori militari leggono le mappe, era un silenzioso avvertimento che l'architettura operativa non era stata progettata per difendersi da sola.

in condizioni di guerra informatica o elettronica, ma per funzionare in tempo di pace, costantemente monitorati da un avversario vigile.

Un esperto di telecomunicazioni libanese che ha trascorso molti anni gestendo infrastrutture di rete riassume la questione in una frase: "La questione non è dove vengono archiviati i dati, ma chi ha la capacità di far funzionare il sistema quando fallisce". E aggiunge: "Nelle guerre moderne, non è necessario rubare informazioni; è sufficiente capire come funziona il sistema per fermarlo nel momento desiderato".

L'allineamento delle nuvole si sviluppa all'interno di questo squilibrio esistente.

Oracle all'interno di un ecosistema geopolitico

Il posizionamento globale di Oracle accresce la delicatezza della decisione del Libano.

L'azienda è specializzata in ambienti di database aziendali ad alta sicurezza per ministeri delle finanze, catene di fornitura della difesa e istituzioni collegate all'intelligence. La sua infrastruttura opera all'interno degli ecosistemi della difesa statunitense e delle reti di sicurezza alleate.

Secondo **Inside Telecom**, il fondatore miliardario dell'azienda, Larry Ellison, ha mantenuto stretti rapporti con il primo ministro israeliano Benjamin Netanyahu. La dirigenza di Oracle ha pubblicamente affermato l'impegno "inequivocabile" dell'azienda nei confronti di Israele, ed Ellison è stato identificato come un importante donatore politico strettamente legato alla leadership israeliana.

Queste relazioni illuminano l'ecosistema geopolitico in cui opera l'azienda. Quando un'azienda del genere si inserisce nella trasformazione digitale di uno Stato impegnato in un conflitto attivo con Israele, l'allineamento strutturale si interseca con l'asimmetria dell'intelligence in modi che non possono essere liquidati come una coincidenza tecnica.

Lo spostamento "tecnopolare"

L'ordine internazionale è cambiato in modi che pongono le aziende tecnologiche al centro del potere strategico.

Il concetto di "mondo tecnopolare", così come **articolato** di Ian Bremmer, presidente dell'Eurasia Group, descrive un sistema in cui le grandi aziende tecnologiche rivaleggiano con gli stati nazionali in termini di influenza geopolitica, plasmando l'ordine digitale ed esercitando potere su dati, piattaforme e algoritmi.

Negli Stati Uniti, l'evoluzione dal programma Joint Enterprise Defense Infrastructure (JEDI) al Joint Warfighting Cloud Capability (JWCC) ha riflesso la consapevolezza che la supremazia militare nel XXI secolo dipende tanto dalla resistenza computazionale quanto dalla forza cinetica. La Cina ha integrato la propria architettura cloud nazionale in sistemi di comando e controllo basati sull'intelligenza artificiale.

Pertanto, l'architettura cloud costituisce un'infrastruttura strategica al più alto livello di governo. L'integrazione del Libano si sviluppa all'interno di questa trasformazione globale, in cui la resilienza computazionale definisce sempre più la resistenza dello Stato.

Il lungo arco della dipendenza

La descrizione del MoU come gratuito oscura l'arco più lungo dell'allineamento istituzionale.

Formare 50.000 partecipanti in cinque anni all'interno di un'architettura proprietaria crea una forza lavoro calibrata su quell'ecosistema, plasmando il modo in cui i ministeri reclutano i talenti, come vengono prese le decisioni sui software e come le infrastrutture future si espandono lungo linee di compatibilità.

La dipendenza raramente si manifesta attraverso obblighi formali. Prende forma gradualmente, man mano che i sistemi diventano familiari e le alternative diventano più difficili da perseguire.

Persino gli alleati più stretti degli Stati Uniti in Europa hanno riconosciuto i rischi di questa dinamica, investendo massicciamente in alternative open source e inasprendo le leggi sulla protezione dei dati nel tentativo di proteggere la propria autonomia digitale.

Il Libano deve ancora predisporre misure di salvaguardia comparabili che possano proteggere la sua infrastruttura digitale da pressioni legali e strategiche esterne.

Sovranità sotto pressione

L'interazione del Libano con le aziende tecnologiche globali è inevitabile. La modernizzazione amministrativa richiede infrastrutture computazionali, integrazione dell'intelligenza artificiale e sistemi di dati in grado di supportare la governance in tempo reale.

La questione strategica riguarda la sequenza e la preparazione. Il controllo sovrano sull'architettura digitale determina se la modernizzazione rafforza la resistenza istituzionale o approfondisce l'esposizione strutturale.

In una regione dove **il vantaggio militare** israeliano è inseparabile dall'integrazione dell'intelligence, l'allineamento architettonico comporta conseguenze geopolitiche.

L'infrastruttura cloud costituisce oggi il quadro attraverso il quale operano i sistemi fiscali, le agenzie di sicurezza si coordinano e la governance persiste durante le crisi. Uno Stato che si integra in ecosistemi digitali governati dall'esterno, senza garanzie sovrane parallele, restringe il proprio margine di autonomia e aumenta la propria esposizione alla leva finanziaria esterna.

Il Libano sta raggiungendo un punto in cui la trasformazione digitale e la sicurezza nazionale non possono più essere trattate come due binari separati.

Ciò che accadrà in seguito dipenderà dalla capacità dello Stato di creare le garanzie legali e tecniche necessarie per mantenere il controllo della propria infrastruttura digitale, anziché consentire che venga plasmata da poteri esterni che già influenzano l'equilibrio di potere della regione.