

La geografia invisibile del potere israeliano

di Lorenzo Maria Pacini

Fonte: Strategic Culture Foundation

La sovranità sui dati è il nuovo petrolio: ma l'Asia occidentale estrae la materia prima, mentre i giganti tecnologici stranieri la raffinano.

La mappa nascosta dai server e l'illusione dei confini digitali

Il 10 giugno 2025, due dirigenti di Microsoft France si sono presentati davanti a una commissione d'inchiesta del Senato francese incaricata di esaminare gli appalti pubblici e la sovranità digitale. L'audizione procedeva secondo il consueto registro rassicurante fino a una domanda che ne ha rovesciato il tono: l'azienda poteva garantire che i dati dei cittadini francesi, anche se ospitati su server collocati in Francia, non sarebbero mai stati trasferiti a un'autorità straniera senza il consenso del governo di Parigi? Anton Carniaux, direttore degli affari pubblici e legali della filiale, ha risposto sotto giuramento con sei parole: «No, non posso garantirlo». La frase ha attraversato anni di lessico aziendale costruito attorno a espressioni come «regioni cloud locali», «infrastruttura affidabile», «residenza del dato». La Francia poteva ospitare i server, i cittadini francesi potevano generare i dati, le istituzioni francesi potevano pagare il servizio: l'autorità ultima, tuttavia, poteva continuare a esercitarsi altrove. La commissione ne ha tratto una conclusione netta. Microsoft non era in grado di garantire la sovranità sui dati che ospitava. Da quello scambio emerge una realtà con conseguenze precise anche, e forse soprattutto, per l'Asia occidentale: la collocazione fisica di un dato non coincide più con la sua collocazione politica.

La geografia classica del potere insegna che la sovranità occupa il territorio. Il petrolio appartiene allo Stato sotto il cui suolo giace; i porti ricadono sotto l'autorità del Paese sulle cui coste sorgono; gli oleodotti rispondono alle frontiere che attraversano. Il potere si legge, in questa tradizione, sulla superficie della terra. Il dato segue una geografia diversa. Una cartella clinica può essere prodotta a Riyadh, archiviata in Bahrein, elaborata da un algoritmo addestrato negli Stati Uniti e amministrata attraverso una filiale europea. Quale Stato la controlla davvero? La risposta

convenzionale attribuisce il dato all'individuo, all'impresa o al governo che lo ha generato. Nella pratica, la proprietà conta meno del controllo. Il potere reale appartiene a chi è in grado di accedere, elaborare, trasferire, restringere o imporre per via legale la divulgazione dell'informazione. Il principio è enunciato senza ambiguità dallo stesso Dipartimento di Giustizia statunitense. In forza del CLOUD Act, i fornitori soggetti alla giurisdizione americana possono essere obbligati a consegnare i dati mediante procedimento legale valido, «*indipendentemente dal luogo in cui l'impresa li conserva*». Washington presenta la norma come strumento legittimo per acquisire prove elettroniche. Sul piano geopolitico, essa consente alla giurisdizione statunitense di viaggiare attraverso il controllo societario, raggiungendo informazioni custodite ben oltre il territorio degli Stati Uniti. La nuova mappa del potere non è disegnata soltanto da confini, cavi e centri di calcolo, ma da sedi legali, chiavi di cifratura, obblighi giuridici, amministratori di sistema e dagli Stati capaci di costringerli a collaborare.

In tutta l'Asia occidentale i governi stanno investendo con decisione in cloud computing, intelligenza artificiale, identità digitale, città intelligenti e servizi pubblici fondati sui dati. L'Arabia Saudita punta a diventare un'economia dei dati di primo piano; Emirati Arabi Uniti, Qatar, Bahrein, Oman e Turchia stanno ampliando le proprie capacità di gestione e governo dell'informazione. Anche la capacità fisica si concentra in pochi poli regionali: una valutazione della Banca Mondiale del 2025 contava trentanove data center negli Emirati e trentatré in Arabia Saudita, cifre inferiori alla media dei Paesi ad alto reddito (ottantuno) ma nettamente superiori al resto dell'area.

La transizione è misurabile. Secondo l'Unione internazionale delle telecomunicazioni, nel 2024 il settanta per cento della popolazione degli Stati arabi utilizzava Internet, contro il 68% a livello mondiale. La media regionale nasconde però un divario di ottantadue punti percentuali tra l'economia meno connessa e quella più connessa, mentre gli abbonamenti a banda larga fissa restano sotto la metà del dato mondiale. L'espansione digitale è rapida e, allo stesso tempo, profondamente diseguale.

La base dei fornitori è invece assai concentrata. Secondo Synergy Research Group, nel terzo trimestre del 2025 Amazon, Microsoft e Google hanno assorbito il sessantatré per cento della spesa mondiale delle imprese in infrastrutture cloud, in un mercato trimestrale salito a centosette miliardi di dollari dai sessantotto di appena due anni prima. Gli Stati che costruiscono in fretta i propri sistemi digitali entrano in un mercato già strutturato attorno alla dipendenza. Un governo può imporre che i dati dei cittadini restino entro i confini nazionali e affidare al contempo a un'impresa straniera la gestione della piattaforma, l'aggiornamento del software, la

fornitura del modello di IA o il controllo degli strati critici del sistema. Ne nasce l'apparenza della sovranità senza la sua sostanza.

La localizzazione del dato risponde a una sola domanda: dove è conservata l'informazione. Lascia aperte quelle decisive. Chi controlla le chiavi di cifratura? Chi aggiorna il software? Chi può sospendere il servizio? La legge di quale Paese governa il fornitore? Chi può imporne la divulgazione, e chi possiede la potenza di calcolo necessaria a estrarne valore strategico? Tenere i server dentro i confini nazionali non li pone sotto controllo nazionale.

La Palestina e i dati come arma

In nessun luogo le conseguenze di questa geografia nascosta appaiono con maggiore evidenza che nella Palestina occupata. La guerra contemporanea dipende sempre più dalla raccolta, dall'incrocio e dall'interpretazione di enormi quantità di informazione. Tabulati telefonici, identificatori biometrici, comunicazioni intercettate, cronologie di localizzazione e immagini aeree possono trasformarsi in intelligence militare attraverso il calcolo in cloud e l'intelligenza artificiale.

L'uso combinato di prodotti Microsoft e OpenAI da parte dell'apparato militare israeliano, nel marzo 2024, aveva raggiunto un livello quasi duecento volte superiore a quello della settimana precedente il 7 ottobre 2023. I dati archiviati sui server Microsoft erano più che raddoppiati, superando i tredici virgola sei petabyte entro il luglio 2024, mentre l'impiego dei server di calcolo cresceva di quasi due terzi nei primi due mesi di guerra. La piattaforma Azure sarebbe stata usata per compilare, trascrivere e tradurre informazioni ottenute mediante sorveglianza di massa, con una parte dell'intelligence incrociata con i sistemi di individuazione degli obiettivi.

Nel settembre 2025 Microsoft ha disattivato alcuni servizi cloud e di IA forniti a un'unità militare israeliana, dopo che una verifica interna aveva accertato l'uso dei suoi prodotti per la sorveglianza di massa dei palestinesi; i dati in questione risultavano conservati in strutture cloud dell'azienda situate in Europa. La catena è istruttiva: informazioni raccolte in Palestina, elaborate da un'unità militare israeliana, ospitate in Europa e infine soggette a una decisione presa da una società statunitense. Il limite del provvedimento lo è altrettanto. Come ha osservato Hossam Nasr, ex dipendente Microsoft e promotore della campagna *No Azure for Apartheid*, la parte prevalente del contratto con l'apparato militare israeliano è rimasta intatta. Le grandi imprese tecnologiche occupano ormai posizioni un tempo riservate quasi esclusivamente agli Stati: forniscono capacità impiegate in operazioni di intelligence, decidono se un cliente conserva l'accesso, indagano sul presunto abuso e impongono restrizioni oltre i confini.

Israele stesso riconosce l'importanza strategica del controllo sul cloud.

Il progetto Nimbus, assegnato a Google e Amazon Web Services, è stato concepito per dotare i ministeri israeliani e gli enti pubblici collegati di un'infrastruttura cloud completa. L'appalto, del valore di un miliardo e duecento milioni di dollari, richiedeva infrastrutture locali ed era presentato come strumento per trattenere l'informazione governativa entro il territorio dello Stato. I fornitori principali restano però società statunitensi, incardinate nei sistemi giuridici e tecnologici americani.

Nimbus incarna il paradosso centrale della sovranità del dato: un governo può esigere che l'informazione rimanga sul proprio territorio e affidarne archiviazione, calcolo e gestione della piattaforma a imprese la cui sede è altrove. Israele ha negoziato con durezza per ridurre questa vulnerabilità. La maggior parte degli Stati dell'Asia occidentale non dispone del suo potere contrattuale, né della sua integrazione tecnologica con Washington, né della sua capacità di pressione sulle grandi imprese americane. La sovranità, qui, è anche una funzione della forza negoziale.

La contesa sui dati è in ultima analisi una lotta su tre diritti strategici. Il primo è il diritto di raccogliere: governi, piattaforme digitali, operatori di telecomunicazioni, banche e servizi di sicurezza accumulano informazioni su identità, movimenti, comunicazioni, salute, consumi e comportamenti. Il secondo è il diritto di calcolare: il dato grezzo acquista valore strategico solo se l'attore possiede i chip, gli algoritmi, le piattaforme cloud e il personale qualificato necessari a elaborarlo. Il terzo è il diritto di imporre: la facoltà, rivendicata da governi e tribunali, di costringere i fornitori a divulgare, conservare, rimuovere o restringere l'informazione.

La concentrazione economica dietro questi tre diritti si intensifica. L'UNCTAD riferisce che le cinque maggiori multinazionali digitali hanno portato la propria quota congiunta delle vendite di settore dal ventuno per cento del 2017 al quarantotto per cento del 2025, mentre la quota di attivi saliva dal diciassette al trentacinque per cento. Il controllo su dati e calcolo si accumula più rapidamente di quanto l'infrastruttura si diffonda. Un Paese che controlli soltanto il primo diritto è un fornitore di materia prima digitale; uno che controlli raccolta e calcolo può diventare una potenza digitale; un attore capace di esercitare tutti e tre possiede qualcosa di prossimo alla sovranità digitale.

La posta economica cresce con rapidità. L'UNCTAD stima che il mercato mondiale dell'intelligenza artificiale passi da 189 miliardi di dollari nel 2023 a 4800 miliardi nel 2033, un incremento di venticinque volte in un decennio. Le regioni che forniscono dati ma difettano dell'infrastruttura di calcolo e della proprietà intellettuale necessarie a elaborarli rischiano di trattenere solo una porzione minima di quel valore. Nel Novecento il valore strategico non risiedeva soltanto nell'estrarre il petrolio, ma nel raffinarlo, trasportarlo,

quotarlo e finanziarlo. Nel XXI secolo la stessa distinzione vale per i dati: l'Asia occidentale può generare la materia prima, ma il potere decisivo abita nelle raffinerie del dato, cioè nelle piattaforme cloud, nei modelli di IA e nei sistemi di calcolo che convertono l'informazione in profitto, intelligence e leva geopolitica.

Oltre il colonialismo digitale

La soluzione non è l'isolamento tecnologico. Nessuno Stato dell'Asia occidentale può riprodurre da solo ogni strato dello *stack* tecnologico globale, e sostituire la dipendenza dai fornitori statunitensi con un'affidabilità totale verso piattaforme cinesi o di altra provenienza sposterebbe soltanto il centro di gravità esterno. Il rischio da evitare è che l'uscita dalla dipendenza petrolifera si converta in colonialismo digitale: un assetto in cui le società della regione generano i dati mentre le piattaforme straniere possiedono l'infrastruttura, ne estraggono il valore e trattengono il potere di accesso. Ciò che serve è un'autonomia tecnologica distribuita. Su questa base si può indicare un ordine di priorità concreto. L'acquisto di servizi cloud va trattato come decisione di sicurezza nazionale, non come routine informatica: i contratti devono stabilire chi controlla le chiavi di cifratura, come saranno gestite le richieste legali straniere, se dati e applicazioni possano migrare verso un altro fornitore. I dati sanitari, difensivi, biometrici, giudiziari e anagrafici richiedono una protezione più severa dell'informazione commerciale ordinaria. I governi devono investire in capacità cloud regionali interoperabili, standard aperti, verifica indipendente e nella possibilità di mantenere i servizi essenziali qualora un fornitore straniero revocasse l'accesso. Soprattutto, la sovranità del dato deve estendersi oltre l'archiviazione fino all'intera catena: raccolta, classificazione, calcolo, accesso, condivisione e cancellazione. Per oltre un secolo l'importanza geopolitica dell'Asia occidentale è stata cartografata attraverso giacimenti, oleodotti, porti, stretti e basi militari. Quelle strutture restano centrali, ma sopra di esse si è disteso un altro reticolo strategico, fatto di banche dati, contratti cloud, giurisdizioni legali, sistemi di identità, modelli di IA e autorizzazioni invisibili. Il controllo sui dati conferisce a Stati e imprese il potere di mappare le società, interpretarne i comportamenti, anticiparne gli spostamenti politici ed economici e tradurre quella conoscenza in azione. Gli Stati dell'Asia occidentale stanno costruendo con rapidità l'infrastruttura digitale su cui poggeranno le loro economie e le loro istituzioni pubbliche. Gran parte dell'autorità che governa quei sistemi rimane però al di fuori della regione. Nel XXI secolo il controllo del territorio dipenderà sempre più dal controllo dei dati che rendono visibili i suoi popoli, le sue istituzioni e le sue risorse.

La domanda posta al Senato francese nel giugno 2025 vale, con ogni evidenza, ben oltre la Francia: chi non può garantire dove finiranno i propri dati non governa fino in fondo il proprio territorio. E con quei dati potrà essere fatto letteralmente qualsiasi cosa.