



CYBER E TECH

La geografia del cyberspazio

Cavi sottomarini, Data Center e Cloud Service Provider: tra connettività e competizione

A cura di Alessia Sposini e Mattia Patriarca

20 FEBBRAIO 2021

L'avvento del cyberspazio non ha cancellato la geografia, l'ha riconfigurata. Un ruolo di spicco è, infatti, giocato dai cavi sottomarini che ricalcano le principali rotte commerciali navali e tracciano l'ossatura di Internet. Lungo queste arterie, si collocano i grandi fornitori di servizi di stoccaggio, conservazione ed elaborazione dei dati. Cosa accade, però, quando non solo le infrastrutture attraverso le quali passa e viene conservato il 99% dei dati, ma anche i contenuti attraverso i quali quei dati vengono generati, sono nelle mani di un solo attore?

La quasi totalità del **traffico internet globale** è veicolata via mare attraverso cavi sottomarini in fibra ottica. Per la precisione si tratta del 99% dei dati scambiati nel mondo¹, dato che fa dei cavi sottomarini la struttura portante della rete internet globale e l'ossatura dell'economia globalizzata. Le connessioni planetarie fanno affidamento su queste infrastrutture per la loro efficienza e la loro convenienza economica: sono meno costose dei satelliti, hanno spesso carattere transnazionale ed hanno un'elevata capacità in termini di *terabytes*.

Se il veicolo delle connessioni globali sono i cavi sottomarini, i principali **luoghi fisici di stoccaggio**, condivisione ed elaborazione **dei dati** trasmessi sono rappresentati dai data center e, in particolar modo, dai *cloud service providers*. Si tratta di aziende private che gestiscono i dati di miliardi di utenti (pubblici e privati) su scala globale. Quando, poi, i fornitori di servizi cloud sono anche *content providers* come Google, Amazon e Microsoft ad essere minacciata è la sovranità digitale degli Stati o, quantomeno, vi è un'evidente disparità di potere nella gestione delle infrastrutture critiche.

Cavi sottomarini

La distribuzione
geografica

I cavi sottomarini in fibra ottica iniziano a connettere paesi e continenti a partire dagli anni '80. Nel **1988** fu posato il primo cavo, il **TAT-8**, che collegava Stati Uniti, Regno Unito e Francia. Da allora si stima che la rete sottomarina in fibra ottica sia cresciuta fino a contare circa 400 cavi in tutto il mondo. Osservando la loro distribuzione geografica, si può notare come questi cavi ricalchino le principali rotte commerciali navali: dalle coste degli Stati Uniti, il paese più collegato del mondo, si propagano numerose direttrici di cavi, rivolte verso l'Europa e la regione Indo-pacifica. Molto traffico è il **Mar mediterraneo**, attraversato da numerosi cavi che entrano nel Mar Rosso per poi raggiungere l'Estremo Oriente ed il Sud-est asiatico attraverso l'Oceano Indiano.

¹ Per informazioni e dati sui cavi sottomarini consultare: www2.telegeography.com

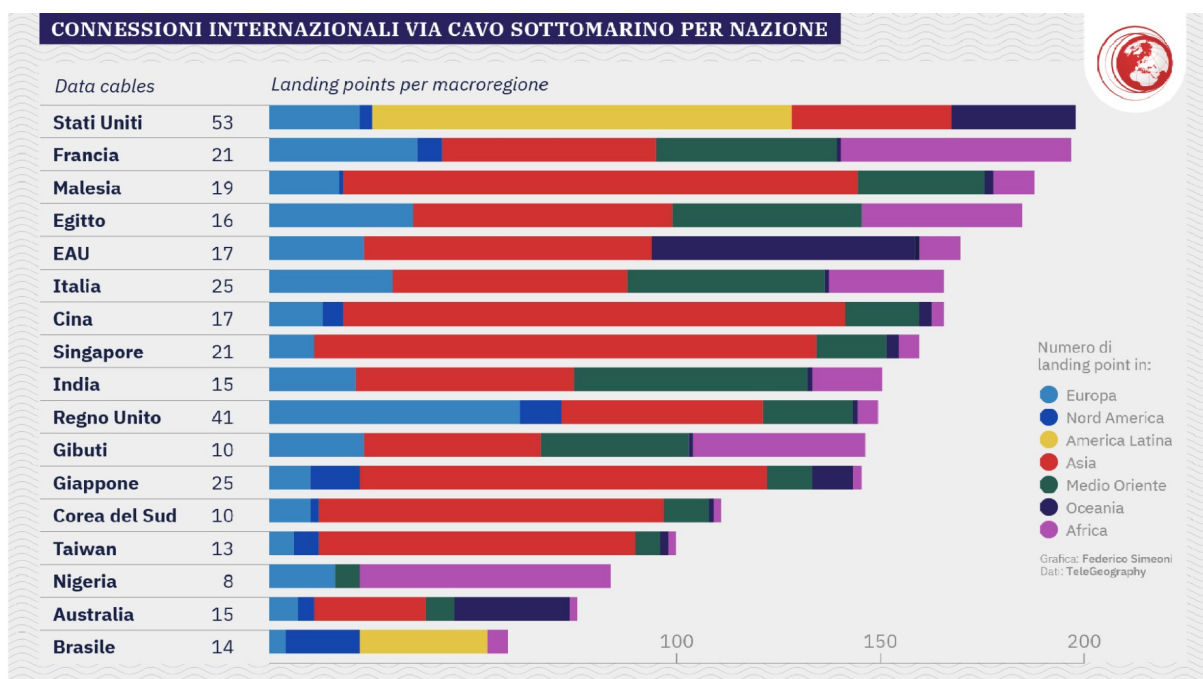


Figura 1: Connessioni Internazionali via Cavo Sottomarino per Nazione

Solitamente la rotta di un cavo non comprende un singolo punto di arrivo, ma prevede molteplici “*landing points*”, letteralmente “punti di attracco”: i cavi spesso si ramificano, sviluppandosi in più direzioni per connettere molteplici località contemporaneamente. Esistono cavi di elevata importanza strategica che collegano più continenti come il **SeaMeWe-3**, il cavo più lungo del mondo con i suoi 39.000 km. Il SeaMeWe-3 collega l’Europa all’Estremo Oriente e l’Australia, passando per l’Oceano Indiano, connettendo un totale di 38 città. Il grafico precedente offre una panoramica sul livello e la distribuzione in termini geografici delle reti di cavi sottomarini dei paesi più connessi a livello mondiale. Accanto al nome di ciascun paese viene riportato il numero totale di cavi che lo collegano sul piano internazionale (non vengono inclusi i cavi meramente nazionali, quelli che collegano diverse sponde dello stesso paese). A fianco a tale numero, per ogni stato vengono graficamente illustrate le regioni ai quali sono più collegati in termini di accessi: è interessante notare quali sono le aree del globo dove un paese dispone di più *landing points* tramite i suoi cavi. Possiamo quindi notare come l’America Latina dipenda ancora in gran parte dalla rete statunitense, o anche come la Francia sia il paese europeo più collegato al continente Africano.

Chi controlla i cavi

Più che la volontà statale, a muovere lo sviluppo del cablaggio sottomarino è prevalentemente l'**investimento privato**: le compagnie scelgono le tratte più rilevanti, quelle che mettono in connessione i principali bacini di utenze. Per questo motivo, negli ultimi anni la regione con più investimenti in tale settore è stata anche quella con il più alto tasso di crescita demografico, ovvero la regione Indo-pacifica². Oggi questi cavi appartengono per lo più a consorzi di aziende private: un singolo cavo è di proprietà di tutte le aziende che hanno contribuito alla sua progettazione e realizzazione. Le aziende sono spesso della stessa nazionalità dei paesi che beneficino della connessione portata dal cavo, ma possono essere anche aziende di caratura internazionale che investono in aree diverse da quella del proprio paese d'origine, come l'americana AT&T o l'indiana TATA Communications. Tale è l'importanza di questi cavi che anche i **Big Tech** americani hanno cominciato a progettare e possedere i propri cavi sottomarini: Google, Facebook, Amazon e Microsoft hanno di recente cominciato a posare i loro cavi, di cui sono proprietari parziali o in alcuni casi unici proprietari. È il caso di Google che possiede i cavi Curie (Stati Uniti-Panama-Cile), Dunant (Stati Uniti-Francia) e Junior (Brasile)³. Proprio Google è il promotore di un progetto che riguarda da vicino l'Italia, il **Blue Raman**: un cavo che collegherà Genova e Mumbai passando per Israele e Arabia Saudita e che vedrà la partecipazione di Telecom Italia Sparkle, la società sussidiaria di Telecom Italia che si occupa delle installazioni sottomarine in fibra ottica.

Rilevanza geopolitica

Nonostante la loro importanza, questi cavi sono essenzialmente **vulnerabili**. La loro grandezza si aggira attorno ai 25 ml e sono esposti a numerosi rischi, dalle calamità naturali alle ancore delle navi, fino ai danni volontari perpetrati dall'uomo. Nel marzo del 2013, la guardia costiera egiziana sorprese tre sub intenti nel tagliare un cavo al largo di Alessandria. Sebbene la motivazione dei sub non fu resa nota, l'evento dimostrò quanto queste infrastrutture siano tanto precarie quanto importanti. Per questo, oltre la pro-

² Submarine Telecoms Forum (2019). *Submarine Telecoms Industry Report*. (<https://subtelforum.com/products/submarine-telecoms-industry-report/> ultimo accesso: 19/02/2021)

³ J. Miller (2019). *This is What Our 2019 Submarine Cable Map Shows Us About Content Provider Cables*. (<https://blog.telegeography.com/this-is-what-our-2019-submarine-cable-map-shows-us-about-content-provider-cables> ultimo accesso: 19/02/2021)

gettazione e la manutenzione, è importante poter fare affidamento su una vasta rete di cavi, in modo da poter minimizzare la portata di un eventuale danno. Il danneggiamento di un cavo potrebbe causare l'interruzione del flusso di dati, ma anche il solo rallentamento di tale flusso potrebbe risultare esiziale per operazioni finanziarie e comunicazioni militari, soprattutto in momenti di crisi e di conflitto.

L'importanza economica e strategica di questi cavi li ha posti spesso al centro di dispute di natura geopolitica, che hanno visto il coinvolgimento di aziende e governi. Caso lampante è quello del **Pacific Light Cable Network (PLCN)**⁴, progettato da Facebook e Google nel 2016 per connettere Stati Uniti, Filippine, Taiwan e Hong Kong. Il progetto incontrò nel 2020 l'opposizione del governo americano, in quanto la tratta Los Angeles-Hong Kong era ritenuta rischiosa: il timore riguardava la possibilità che tramite il collegamento con Hong Kong il governo cinese potesse avere un canale di accesso ai dati statunitensi, soprattutto dopo che l'autonomia della città a statuto speciale è stata messa in dubbio dai recenti avvenimenti. Lo sforzo dei governi quindi è quello di riuscire a convergere con le aziende per tutelare la sicurezza nazionale ed evitare progetti che possano esporre potenzialmente i propri dati a minacce esterne.

Altro obiettivo strategico riguarda la **differenziazione** del proprio **network** di cavi, disporre di molteplici rotte in modo da non dipendere dalle connessioni che attraversano un determinato paese. Il Brasile, ad esempio, disporrà nel 2021 di EllaLink, un cavo che collega direttamente il paese all'Europa, con l'obiettivo implicito di fornire un accesso alla rete del vecchio continente senza passare per i cavi statunitensi, sui quali l'America Latina dipende in gran parte per le connessioni intercontinentali⁵. Esemplificativo è anche il già citato progetto Blue Raman: la particolarità della rotta disegnata da Google sta nell'evitare l'Egitto, la cui instabilità politica rappresenta una potenziale minaccia per i numerosi cavi che già lo attraversano.

⁴C. Rossi (2020). *Perché è naufragato il cavo sottomarino di Google e Facebook verso Hong Kong*, Start Magazine. (<https://www.startmag.it/mondo/perche-e-naufragato-il-cavo-sottomarino-di-google-e-facebook-verso-hong-kong/> ultimo accesso: 19/02/2021)

⁵ G. Suffia (2018). *Geografia delle cyberwars*, Milano, Giuffrè Editore, pp. 58-59.

Il caso italiano

Come è posizionata l'**Italia** nella mappa dei cavi? L'Italia ha in realtà una posizione di prim'ordine, è uno dei paesi più connessi a livello globale, per la precisione tra i primi tre. In particolare, è la Sicilia a giocare il ruolo di hub internazionale dei cavi, essendo posta al centro del Mediterraneo, mare di passaggio per la rete del cablaggio internazionale. Le città di Palermo, **Mazara del Vallo** e Catania fungono da *landing point* per cavi di portata intercontinentale, come il già citato SeaMeWe-3, o anche l'IMEWE che collega Italia, Egitto, Emirati Arabi Uniti e India, o il FLAG Europe-Asia (FEA), che si estende dal Regno Unito al Giappone, passando per l'Italia. Nonostante la posizione geografica favorevole, l'Italia si trova ad affrontare diverse sfide nel campo della connettività in fibra ottica. Le aziende, per installare un cavo, ricercano determinati requisiti che possano rendere conveniente la sua realizzazione. Per questo motivo, negli ultimi anni la città francese di Marsiglia ha attratto sempre più investimenti in cavi, grazie al preesistente ecosistema digitale, al minor costo dell'energia, ma soprattutto grazie all'assenza di ostacoli burocratici, ancora troppo frequenti invece per chi vuole investire in Italia. Al momento, **Marsiglia** è il principale polo mediterraneo dei cavi sottomarini, catalizzando la maggior parte dei flussi di dati provenienti da oriente. Per sfruttare al meglio la sua posizione strategica, l'Italia dovrà beneficiare di politiche adeguate, volte alla semplificazione burocratica e in grado di incentivare la formazione di realtà digitali in grado di attirare investimenti in termini di connettività⁶.

⁶ Per approfondire: E. Verga (2018). *Nuove rotte digitali: il caso Marsiglia e le opportunità da cogliere in Italia*, Il Sole24 Ore.
(<https://www.econopoly.ilsole24ore.com/2018/12/12/rotte-digitali-marsiglia-italia/>
ultimo accesso: 19/02/2021)

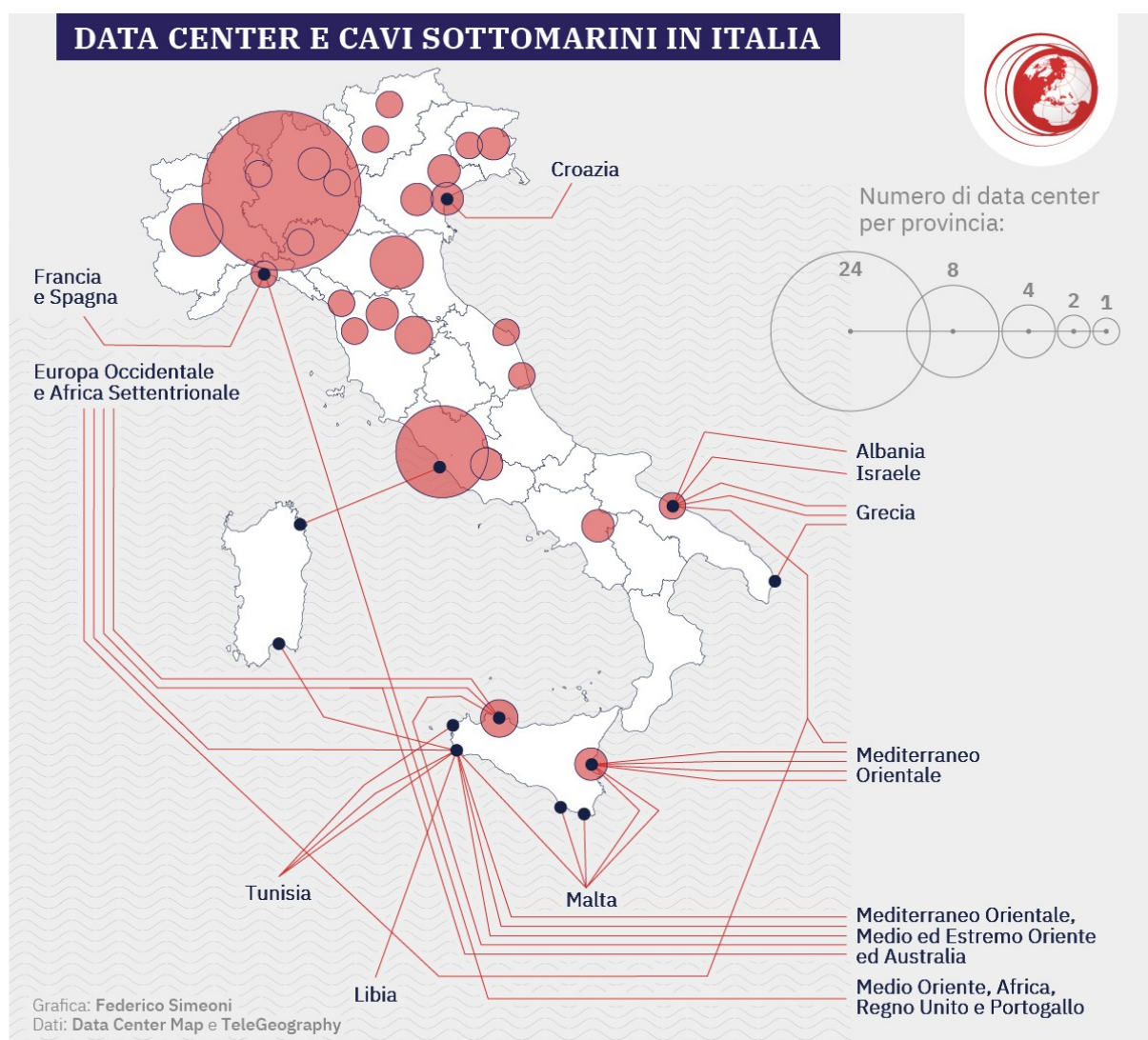


Figura 2: Data Center e Cavi Sottomarini in Italia.

La Figura 2 propone una mappa geografica dell'infrastruttura digitale italiana, tracciando le rotte dei cavi sottomarini che collegano l'Italia al resto del mondo: molti sono i collegamenti verso il Medio Oriente ed il Nord Africa, ma il bel paese risulta un importante polo connettivo anche per i Balcani e la Grecia con i cavi che partono dalla città di Bari. La stessa mappa illustra la distribuzione sul territorio italiano di un'altra infrastruttura digitale fondamentale, il data center, che sarà oggetto dei prossimi paragrafi. La presenza di data center è indicativa di un **ecosistema digitale**: testimonia uno sviluppo economico e tecnologico e, con le giuste politiche, può portare a percorsi virtuosi in termini di innovazione.

Data Center e Cloud Service Providers

La distribuzione geografica

I data center, anche detti CED (**Centri Elaborazione Dati**), sono il fulcro infrastrutturale delle comunicazioni e dei servizi di rete⁷; essi ospitano server, *storage*, gruppi di continuità e via discorrendo. Tutta l'infrastruttura di un data center è incentrata su reti che implementano il protocollo IP e collegano tra loro macchine e applicazioni⁸.

I principi generali della localizzazione dei data center riguardano: la stabilità geopolitica del territorio, l'instabilità politica di un Paese genera un rischio di potenziale distruzione dell'infrastruttura che, di conseguenza, verrà edificata altrove, in un territorio a "basso rischio"; la prossimità alle utenze; in prossimità di fonti energetiche che abbassino la spesa energetica di raffreddamento⁹; in prossimità di mano d'opera specializzata.

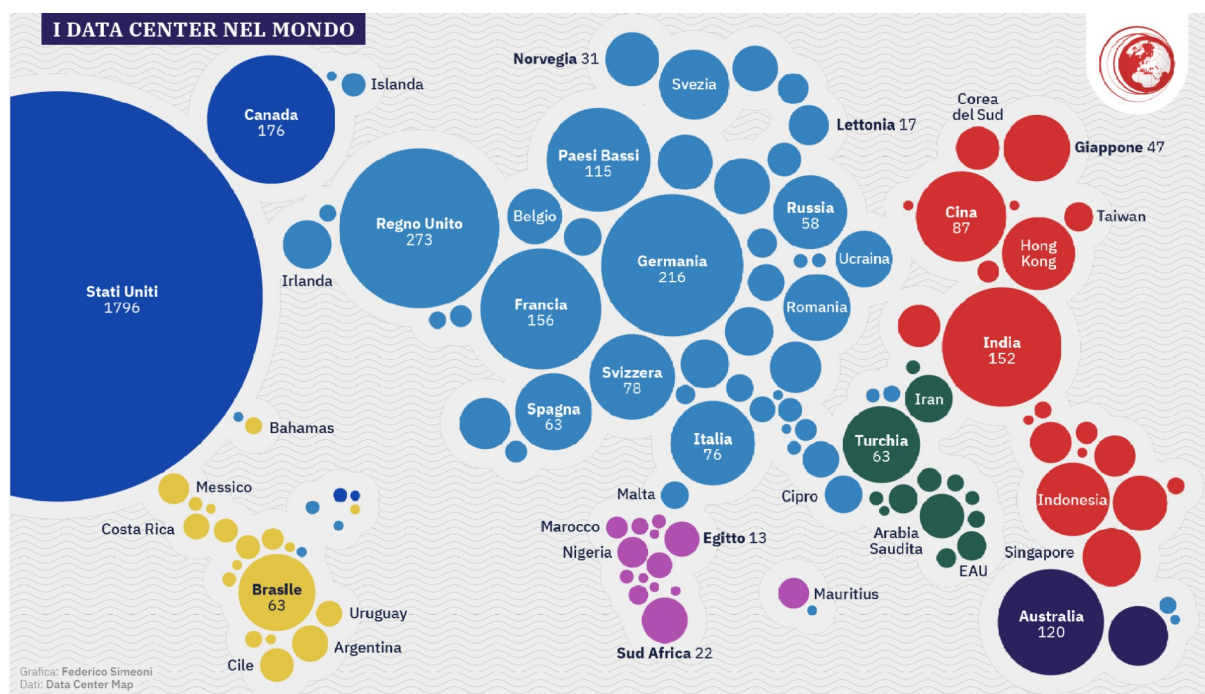


Figura 3: I Data Center nel Mondo. Nella stima effettuata compaiono solo i data center dichiarati, per tanto i numeri effettivi potrebbero discostarsi dal grafico

⁷ Lo Russo, L., Bianchi, E. (2016). *Sistemi e Reti 2*. Milano: Hoepli.

⁸ Ogni *server farm* ospita differenti set di *router* (dei dispositivi di rete che si occupano di instradare i dati, suddivisi in pacchetti, fra sotto-reti diverse) e *switch* progettati e configurati per veicolare il traffico dati in modo bidirezionale fra i server e il resto del mondo.

⁹ D. Barbera (2017). *Siamo stati a vedere dove Facebook conserva i tuoi dati: al fresco, ai confini del Circolo Polare Artico*, Wired.it. (<https://www.wired.it/internet/web/2017/06/30/data-center-facebook-lulea-circolo-polare-artico/> ultimo accesso: 19/02/2021)

La distribuzione geografica dei data center per paese, così come rappresentata nella Figura 3, indica una prevalenza, pari al 38,1% sul totale, di infrastrutture negli Stati Uniti. Le capacità statunitensi, in termini di infrastrutture possedute, sono superiori a quelle dell'Europa che rappresenta 33,5% dei data center totali. Volendo considerare la distribuzione geografica, il Nord America detiene infatti il 41,8% dei data center a livello mondiale. L'Italia conta, invece, l'1,6%¹⁰ dei data center globali, superata in Europa da Regno Unito, Germania, Francia e Svizzera. La collocazione è ripartita su 126 paesi, per un totale di 4714 data center.

Il graduale **passaggio** – ad oggi ancora in atto – dai data center proprietari al *cloud computing* ha portato ad un cambiamento di paradigma tecnologico, passando dalle infrastrutture come prodotto alle infrastrutture come servizio. La componente *hardware* dei data center perde progressivamente importanza, con il *cloud computing* l'equipaggiamento fisico è reso accessibile, a chiunque e in qualsiasi momento, tramite il *software-based management*. L'immediatezza di accesso ai servizi e la condivisione delle risorse fisiche della “nuvola” hanno reso ridefinito l'importanza della collocazione geografica dei data center, quando si fa riferimento alla possibilità di utilizzo. La geografia del cloud, tuttavia, dimostra invece avere rilevanza geopolitica e strategica, come si vedrà più avanti.

Quando si fa riferimento al *cloud computing*, in realtà non si tratta di un servizio unico, ma di – prevalentemente – tre modelli distinti in base al servizio offerto:

- Saas o ***Software as a Service***, si tratta di servizi basati sul web, applicazioni delle quali non si ha la proprietà, ma un modulo di abbonamento.
- IaaS o ***Infrastructure as a Service***, è il modello che permette l'utilizzo delle infrastrutture fisiche del *cloud provider* (server, gruppi di continuità, raffreddamento...) come se fossero un servizio, appunto, e non un prodotto. Alcuni *providers* permettono di scegliere la collocazione geografica del server utilizzato, mentre l'interazione con quest'ultimo avviene tramite macchine virtuali, o VM *virtual machines*.

¹⁰ Vedi figura 2 per la distribuzione dei data center sul suolo italiano.

- PaaS o **Platform as a Service**, oltre alla fornitura delle infrastrutture fisiche viene integrata la gestione della piattaforma (ambiente virtualizzato, framework di sviluppo, monitoraggio e sicurezza). La componente software può essere amministrata liberamente dall'utente.

Quando si fa riferimento al cloud, un'altra distinzione in atto è quella tra *private* e *public* cloud. Il cloud cosiddetto privato è l'opzione meno comune – visti i costi elevati –, le risorse informatiche sono dedicate a un soggetto che, generalmente, associa a questo tipo di servizio anche un'infrastruttura di rete privata per una maggiore sicurezza nella trasmissione e nella gestione delle comunicazioni. Il cloud pubblico, dunque, riguarda tutto il resto, e cioè la condivisione di risorse con più utenti, pur non interagendo mai con essi. È possibile una fusione tra le due modalità sopra descritte, che porta all'*hybrid* cloud.

Un anno di svolta per il **cloud computing** è stato il **2006**, anno in cui Amazon Web Service (AWS) – società nata dalla famosa piattaforma di e-commerce Amazon.com – diede la luce a S3, *Simple Storage Service*, per lo stoccaggio dei dati e EC2, *Amazon Elastic Compute Cloud*, per l'affitto di macchine virtuali. Entrambi i servizi cloud furono resi disponibili prima, nel 2006, negli Stati Uniti e nel 2007 fecero il proprio debutto sul mercato Europeo, da quel momento in avanti la presenza di AWS è in continuo crescendo su scala globale. La modalità prevalente di rendimento del *cloud computing* si attesta, nel 2019, al SaaS con 102.1 miliardi di \$, seguita dalla IaaS con 44.5 miliardi di \$ e dalla PaaS con 37.5 miliardi di \$¹¹.

Chi controlla il Cloud?

Chi sono i *providers* del *cloud computing*? **Amazon Web Services**, **Google Cloud**, IBM Cloud, **Microsoft Azure**, Oracle Cloud e Alibaba Cloud sono i principali fornitori di servizi di cloud pubblico. Nella Figura 4 sono riportati AWS, Google Cloud e Microsoft Azure che di fatto gestiscono non solo gran parte dei servizi cloud globali, ma sono anche i principali fornitori di contenuti, o *content providers*, e da qualche anno a questa parte stanno allargando i propri investimenti in infrastrutture di rete quali i cavi sottomarini¹²,

¹¹ T. Herr (2020). *Four Myths about The Cloud. The geopolitics of cloud computing*. Atlantic Council. (<https://www.atlanticcouncil.org/wp-content/uploads/2020/09/CLOUD-MYTHS-REPORT.pdf> ultimo accesso: 19/02/2021)

¹² R. Miller (2018). *Cloud Players Are Redrawing the Subsea Cable Map*, Data Center Frontier. (<https://datacenterfrontier.com/cloud-players-are-redrawing-the->

come già accennato nel paragrafo precedente. Il trend di espansione delle infrastrutture cloud dei *content providers* riguarda anche i **cloud on-ramps**, o punti di snodo della connettività¹³ globale del cloud.

Nella Figura 4 è illustrata la distribuzione per regioni geografiche sia delle **cloud regions**, la *location* fisica all'interno della quale sono dislocate le risorse dei cloud service providers, e i **cloud on-ramps**, anche detti *cloud exchange*, che permettono di *switchare* i dati da un'infrastruttura all'altra. Questi ultimi, dunque, permettono l'agilità nello spostamento dei dati da una *region* all'altra. L'investimento delle "Big three" in infrastrutture di rete (cavi), rappresenta un passaggio tecnologico quasi "naturale" se si considera che attualmente la maggior parte di traffico internet, almeno nei network Trans-Atlantico e Trans-Pacifico¹⁴, è rappresentato dai *content providers*.

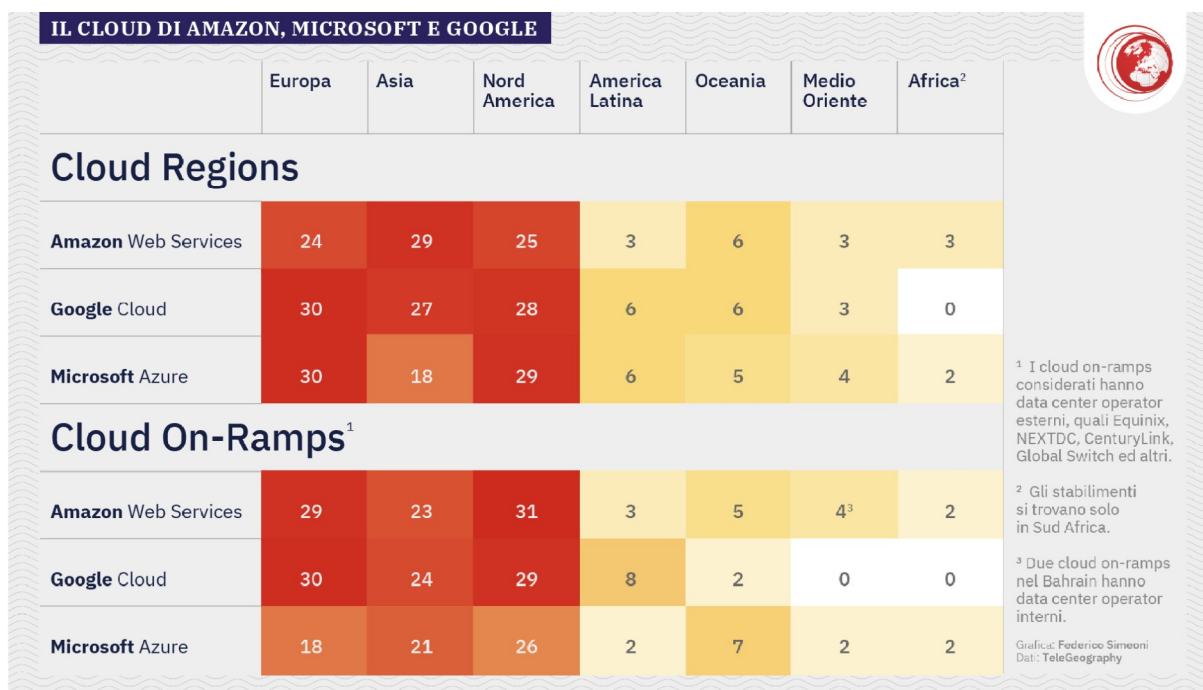


Figura 4: Il Cloud di Amazon, Microsoft e Google.

Tutt'altro discorso è il potenziale geopolitico di questo passaggio tecnologico. Ampliando lo sguardo al risvolto politico di tali investimenti, già nel 2017 Google, Amazon, Facebook, Apple e

[subsea-cable-map/](https://blog.telegeography.com/2021-trends-in-cloud-infrastructure-and-global-networks) ultimo accesso: 19/02/2021)

¹³ P. Christian (2021). *Trends in Cloud Infrastructure and Global Networks*, TeleGeography. (<https://blog.telegeography.com/2021-trends-in-cloud-infrastructure-and-global-networks> ultimo accesso: 19/02/2021)

¹⁴ *Ibidem*

Una questione di
sovranità digitale

Microsoft venivano definite le “**Frightful Five**”¹⁵. Si stima, infatti, che circa l’80% dei dati personali degli utenti che hanno accesso ad Internet siano detenuti dai **GAFAM** e che vengano utilizzati a fini commerciali¹⁶. Amazon, Google e Microsoft dimostrano avere una presenza forte soprattutto in Europa, Asia e Nord America, in termini di infrastrutture cloud, come riportato in Figura 4, e spingono per tanto gli Stati a ragionare in termini di rischio alla sovranità digitale.

L’impiego su larga scala del *cloud computing* come servizio *software* corrisponde alla crescente attenzione da parte della società civile e degli Stati circa la protezione della quale i dati trattati da queste piattaforme godono. La reazione degli Stati si è tradotta in una corsa non solo alla protezione dei dati personali, ma alla localizzazione delle infrastrutture che trattano i dati dei cittadini su suolo nazionale. Un esempio è quello delle ondate di legislazione in materia di **localizzazione dei dati personali** da parte della Federazione Russa, come la Legge Federale 242-FZ¹⁷ che ha reso obbligatorio il salvataggio e la gestione dei dati personali dei cittadini russi entro i confini federali. L’adattamento delle aziende di *cloud computing* alle legislazioni – come il GDPR dell’Unione Europea – e ai mercati regionali, ha garantito la loro espansione su scala mondiale, tuttavia, tale crescita sembrerebbe rappresentare una minaccia alla sovranità tecnologica e digitale degli Stati. In risposta a tale rischio, un caso particolare è costituito dalla nascita di **GAIA-X**¹⁸, un’iniziativa a guida francese e tedesca per un cloud Pan-Europeo. L’intento è quello di mettere in sicurezza i dati europei da compagnie che offrono servizi di *public cloud* come le già menzionate AWS, Microsoft Azure e Google Cloud di derivazione statunitense.

¹⁵ Manjoo, F. (2017). *Tech’s Frightful Five: They’ve Got Us*, New York Times. (<https://www.nytimes.com/2017/05/10/technology/techs-frightful-five-theyve-got-us.html> ultimo accesso: 19/02/2021)

¹⁶ Mainoldi, L. (2018). *Washington e Silicon Valley non si amano ma spiano il mondo insieme*, Limes, Rivista italiana di geopolitica, 10, pp. 53-62.

¹⁷ Federal Law 242-FZ (2014) “On Amending Certain Legislative Acts of the Russian Federation Regarding Specification of the Procedure for Processing personal Data in Information and Telecommunication Networks”

¹⁸ Federal Ministry for Economic Affairs and Energy (2020). *GAIA-X: Policy Rules and Architecture of Standards*. (https://www.data-infrastructure.eu/GAIA-X/Redaktion/EN/Publications/gaia-x-policy-rules-and-architecture-of-standards.pdf?__blob=publicationFile&v=5 ultimo accesso: 19/02/2021)

In tal senso, si tratta di una preoccupazione degli Stati in termini di “*geography of cloud forms*” o ‘Cloud I’, definita da Louise Amoore come “l’identificazione e la collocazione spaziale dei data centres dove si pensa si materializzi il cloud”¹⁹. La distribuzione fisica delle infrastrutture rappresenta una disposizione dei **centri di potere** controllati dai *providers*, la funzione della geografia è quella di identificare tali centri e da tali premesse deriva la possibilità degli Stati di riaffermare la propria giurisdizione mediante interventi legislativi circa il trattamento dei dati e/o la localizzazione delle strutture entro i confini nazionali, il tutto giustificato dalla necessità di una neutralità della rete, che quindi non sia in mano a pochi *providers*.

Un altro discorso è quello che Amoore definisce come ‘Cloud II’ o “*the geography of cloud analytics*” per cui “il *cloud computing* trasforma cosa o chi è reso percepibile e calcolabile”²⁰. In altre parole, gli algoritmi analitici applicati al *cloud computing* portano in superficie i *pattern* sottesi dei dati, trasformandoli in informazioni e investendoli di un significato altrimenti invisibile. Un esempio di come gli stessi *cloud providers* abbiano riconfigurato la possibilità di accesso ai dati in ambito militare e di *intelligence* è da trovarsi nel programma **ICITE**, *Intelligence Community Information Technology Enterprise*, che coinvolge Amazon Web Services e 17 agenzie di *intelligence* statunitensi, tra le quali il Department of Homeland Security, la National Security Agency, la Central Intelligence Agency, il Federal Bureau of Investigation e via discorrendo. Il programma permette la condivisione, il salvataggio e l’analisi dei dati delle agenzie di *intelligence* dando vita a nuove forme di informazione aggregata, che per tale ragione ha un potenziale predittivo pressoché infinito, soprattutto se unita a strumenti di Intelligenza Artificiale che permettono di creare connessioni tra i modelli investigativi delle 17 agenzie²¹. La portata di ICITE aumenta se, oltre ai dati già considerati, si uniscono i dati commerciali degli utilizzatori dei *content providers*.

¹⁹ L. Amoore (2018). *Cloud geographies: Computing, data, sovereignty*, Progress in Human Geography, Vol. 42(1), pp. 4-26.

²⁰ *ibidem*

²¹ L. Amoore, V. Piotukh (2015). *Life beyond big data: Governing with little analytics*, Economy & Society, 44(3), pp. 341-366.

In sintesi, l'influenza dei fornitori di servizi cloud si estende su vari livelli: degli utenti o di protezione dei dati personali, di mercato o geo-economico e di competizione alla sovranità digitale degli Stati o geopolitico. L'intersezione tra connettività, gestione dei dati, produzione dei contenuti – e dei dati generati dagli utenti che utilizzano quei contenuti – investe i providers della forza di ridisegnare il cyberspazio, in termini di confini e di centri di potere. Le zone ad alta penetrazione di questi servizi hanno maggiore sicurezza in termini di accesso alla rete, mentre le zone già rese instabili da condizioni geopolitiche precarie, finiscono per essere ancor più marginalizzate nello scacchiere globale.

Conclusioni

Le infrastrutture digitali rappresentano il veicolo dei dati, quindi di transazioni economiche, comunicazioni e, in generale, scambio di informazioni. In sostanza tutte le relazioni umane fanno ormai riferimento ad esse. La loro spazialità, il loro essere geograficamente collocate, le rende oggetto di contesa. Sicuramente la competizione è in atto tra gli Stati, ma essa è prima di tutto in atto tra il settore pubblico e quello privato: lo sviluppo di cavi sottomarini e data center è trainato dagli investimenti privati e sta ai governi cercare di mediare con aziende e multinazionali del settore, per arginare conflitti e cooperare in materia di *cybersecurity*. Altra considerazione che emerge è il bisogno che la classe dirigente si impegni ad implementare politiche che incentivino lo sviluppo di infrastrutture digitali, volte ad aumentare connettività dei territori. Non solo incentivi economici, ma anche provvedimenti per lo snellimento delle procedure burocratiche, troppo spesso ostacolo per chi vuole investire ed innovare.

Alessia Sposini

Studentessa di Laurea Magistrale presso Sapienza Università di Roma in Valutazione e Ricerca Sociale Applicata. Junior Fellow del Centro Studi Geopolitica.info e responsabile dell'area "Cyber e Tech". Tra i campi di interesse figurano i temi della Sovranità Digitale e dei Diritti Digitali. Co-coordinatrice di Youth IGF Italy, iniziativa giovanile riconosciuta dall'ONU nell'ambito dell'Internet Governance Forum e volta al coinvolgimento dei giovani nel dibattito e nel policy making sulle tematiche del digitale. Membro del Comitato di Programma di YOUTH-DIG2021 e di IGF Italia 2021.

Mattia Patriarca

Laureato magistrale con lode in Scienze della Politica all'Università La Sapienza di Roma, collabora con il Centro Studi da gennaio 2020. All'interno della redazione fa parte dell'area Asia-Pacifico, nella quale si è occupato principalmente di tematiche inerenti agli sviluppi militari nella regione e alla geopolitica del Mar Cinese Meridionale. Altro ambito di interesse è quello della geopolitica delle infrastrutture digitali, sulla quale ha basato la sua tesi magistrale

Il Centro Studi

Il Centro Studi Geopolitica.info nasce nel 2004 con l'obiettivo di offrire un contributo al dibattito sulla politica estera, la geopolitica e le relazioni internazionali dalla prospettiva dell'Italia. Le attività del Centro Studi si articolano in tre filoni principali: la pubblicazione della Rivista online *Geopolitica.info* e la ricerca in materia di politica internazionale e geopolitica; la formazione attraverso i corsi in presenza e i corsi online sulla piattaforma www.onlineducation.it; l'organizzazione di momenti di dibattito pubblico sui temi dell'agenda politica italiana relativi alle relazioni internazionali. Tutte le attività sono consultabili sul sito web www.geopolitica.info.

Centro Studi Geopolitica.info

www.geopolitica.info | centrostudi@geopolitica.info