

## **L'industria del cloud ed il ruolo dell'Italia nell'ambito del progetto Gaia-X**

*a cura di Maurizio Dècina, Alfonso Fuggetta e Antonio Perrucci*

Il paper è il risultato del lavoro di un gruppo di studio e ricerca costituito nell'ambito del Laboratorio sull'Ecosistema Digitale di Astrid, diretto da Antonio Perrucci. La ricerca è stata coordinata da Maurizio Dècina, Alfonso Fuggetta ed Antonio Perrucci. Hanno inoltre partecipato ai lavori del gruppo: Daniele Ali (Fincantieri), Franco Bassanini, Francesco Bonfiglio, Carlo Bozzoli (Enel), Luca Cardone (Retelit), Pier Luigi Dal Pino (Microsoft), Claudio Farina (Snam), Valerio Francola, Giuseppe Italiano, Paolo Lupi, Dario Pagani (Eni), Franco Pizzetti, Federico Protto (Retelit), Franco Spicciariello (Amazon Web Services), Giorgio Veronesi (Snam). Amazon Web Service, Enel, Eni, Fincantieri, Microsoft e Snam hanno contribuito al finanziamento della ricerca.

La responsabilità di quanto sostenuto nel paper è tuttavia esclusivamente di Astrid e dei curatori che lo hanno redatto.

*Il progetto di ricerca si è avvalso della collaborazione in qualità di sponsor di:*



## **Indice**

### **Executive Summary**

### **Premessa**

### **Capitolo 1. L'industria del cloud: profili infrastrutturali, di mercato e di regolazione "tecnica"**

- 1.1. Cloud Computing e Gaia-X
- 1.2. Cenni agli aspetti tecnici dei sistemi di Cloud Computing
- 1.3. I modelli di servizio
- 1.4. Modelli di dispiegamento del cloud
- 1.5. La sicurezza e la resilienza del dato nel Cloud

### **Capitolo 2. La regolazione "giuridico-economica" del cloud: il tema dei dati**

- 2.1. La via "tradizionale" della regolazione dei mercati
- 2.2. La regolazione dei servizi e dei mercati digitali

### **Capitolo 3. L'assetto competitivo del mercato europeo del cloud: possibili evoluzioni**

- 3.1. Un quadro generale
- 3.2. Le determinanti dell'adozione dei servizi cloud da parte delle imprese
- 3.3. Il cloud per la Pubblica Amministrazione: indicazioni per l'esperienza italiana
  - 3.3.1. La storia dell'informatica nella PA: cenni
  - 3.3.2. La razionalizzazione dei servizi informativi delle Amministrazioni Pubbliche

### **Capitolo 4. Prime considerazioni conclusive**

- 4.1. Quale strategia industriale per il cloud europeo: oltre il "campione europeo del cloud"
- 4.2. La natura e il ruolo di Gaia-X

### ***Executive Summary***

*L'idea di promuovere un gruppo di studio sul tema dell'industria del cloud – con specifico riferimento al mercato italiano - nasce sul finire della estate scorsa, quando l'iniziativa denominata Gaia-X attira anche l'attenzione dei media e si comincia a discutere circa i possibili riflessi per il cloud italiano. Dopo un paio di riunioni di brainstorming, viene avviato un gruppo di lavoro formato prevalentemente da manager di imprese fornitrici ed utilizzatrici di servizi cloud, nonché da esperti di diversa formazione (tecnica, economica, giuridica). Dopo alcuni seminari in cui sono state discusse versioni precedenti, è stato predisposto questo testo, che costituisce una base di discussione sia all'interno di Astrid, che con interlocutori esterni, ossia rappresentanti dell'industria e policy makers. All'esito di queste occasioni di confronto ed approfondimento, sarà possibile rivedere il presente rapporto, anche integrando l'analisi con ulteriori dimensioni che non è stato possibile esaminare in questa occasione, come ad esempio il tema delle competenze digitali.*

*Il documento è strutturato in quattro sezioni. La prima – a mo' di introduzione – descrive i profili di natura tecnica ed infrastrutturale, le caratteristiche dell'offerta ed i modelli di servizio, le problematiche legate alla sicurezza, con alcuni cenni alla cosiddetta “regolazione tecnica” del cloud. La seconda sezione costituisce un approfondimento degli aspetti di natura regolamentare, con attenzione tanto al mercato del cloud, quanto a quello dei dati, quest'ultimo oggetto di diversi interventi della Commissione europea. Nella terza sezione, si analizzano gli assetti di mercato dell'industria del cloud, valutandone le possibili traiettorie di sviluppo, alla luce – anche – del progetto Gaia-X. In questo contesto, una attenzione particolare è riservata al cloud della Pubblica Amministrazione. L'ultima sezione, infine, propone alcune considerazioni conclusive che, vengono riassunte di seguito.*

*Sostanzialmente, sono quattro i grandi temi, ossia le domande, che hanno occupato il gruppo di lavoro, il quale, alla fine, è pervenuto ad altrettante risposte, in alcuni casi prospettando più di un'alternativa.*

*La prima questione ha riguardato il tema del “campione europeo” del cloud: un tema mai del tutto esplicitamente rappresentato nell'ambito dei lavori di Gaia-X, soprattutto nella fase iniziale, ma anche ora nell'attuale configurazione di Associazione europea. A sua volta, questo “dilemma” rimanda alla questione di quale sia la collocazione del*

*progetto Gaia-X tra i vari modelli cui potrebbe richiamarsi (trattato più avanti).*

*La prospettiva di un campione europeo nel mercato del cloud, che sfidi i grandi operatori statunitensi e cinesi, mai evocato da Gaia-X, è invece un obiettivo dichiarato dal Commissario Breton, in occasione di interventi a workshop e convegni, soprattutto nell'ambito delle (poco note) attività della European Alliance on Industrial Data and Cloud (AIDC, anche Alleanza).*

*A questo proposito, resta da capire meglio quali siano le relazioni tra le attività delle due iniziative: Gaia-X e la menzionata Alleanza. Su questo passaggio – cruciale – ci si attende un contributo importante dalle occasioni di discussione del paper che qui si presenta. In particolare, riteniamo che quella certa iniziale ambiguità nel progetto Gaia-X in relazione ai profili extra-regolamentari sarà progressivamente risolta con l'operatività stessa dell'Associazione, nonché quando saranno più chiari i rapporti con l'Alleanza di Breton. Con riferimento alla situazione attuale, e sulla base di esperienze precedenti, la conclusione del gruppo di lavoro in merito alla promozione di un campione europeo del cloud è netta: per diverse ragioni, l'ipotesi di costituire un campione europeo in grado di sfidare i grandi operatori americani e cinesi appare velleitaria.*

*In senso contrario ad una tale ipotesi, si ricorda innanzitutto il ritardo di 10-15 anni che l'industria europea del cloud sconta nei confronti dei concorrenti internazionali: ritardo che pare incolmabile, soprattutto per il ritmo che l'innovazione tecnologica continua ad avere in questo settore. Un deterrente a muoversi in questa direzione viene anche dall'esperienza di quei paesi (la Francia) che hanno tentato – senza successo - di costruire un “campione nazionale” del cloud. Vi sono poi da considerare le preoccupazioni per la concorrenza che – plausibilmente – potrebbero essere sollevate dalle autorità antitrust, a livello comunitario e/o nazionale, per la costituzione di un soggetto in grado di ridurre il grado di concorrenza soprattutto a livello di singolo mercato nazionale. Da ultimo, si manifesta una perplessità di carattere “politico” circa la “nazionalità” del campione europeo che, nei fatti, rischierebbe di essere la riproposizione di un campione nazionale, stavolta su scala europea. In ogni caso, il gruppo di lavoro non è pregiudizialmente contrario all'idea che l'intervento pubblico a sostegno dell'industria del cloud e dei dati, in certe circostanze, possa assumere - anche - la forma di un sostegno ad investimenti privati, eventualmente attraverso forme di partnership pubblico/privato.*

*Si viene così ad una seconda questione, che riguarda il nostro Paese più da vicino, perché rappresenta un progetto del precedente Ministro dell'innovazione tecnologica e del digitale: la costituzione di una joint venture pubblico/privata per la fornitura di servizi cloud alla Pubblica Amministrazione, in particolare ad un numero rilevante di*

*grandi pubbliche amministrazioni centrali. Si tratta di un progetto che desta molte perplessità tra i partecipanti al gruppo di lavoro, che non ne comprendono le motivazioni, almeno per quello che si è riusciti a sapere sui contenuti dell'iniziativa.*

*Nel merito, oltre ad osservare che esiste già un fornitore di servizi cloud "specializzato" per la PA (Sogei per le necessità del Ministero dell'Economia e Finanze), si ritiene che questa frammentazione della domanda pubblica di servizi cloud non abbia significato dal punto di vista economico, mentre al tempo stesso amplificherebbe i problemi di interoperabilità dei sistemi.*

*Inoltre, al di là delle dichiarazioni sulla libertà delle amministrazioni pubbliche di scegliere liberamente sul mercato il proprio fornitore, quindi anche un soggetto diverso dalla joint venture, appare evidente che le prospettive di successo di questo nuovo operatore pubblico/privato – qualora vi siano - risultano legate alla possibilità di avere una clientela captive, rappresentata appunto dalle grandi amministrazioni centrali. Il Governo, promotore della joint venture, sarebbe quindi indotto ad esercitare una moral suasion nei confronti delle amministrazioni centrali, che – di fatto – restringerebbe la loro libertà di scelta, e, sicuramente, costituirebbe anche un indirizzo per altre amministrazioni dello Stato.*

*Qualora poi il Governo decidesse comunque di andare in questa direzione, e costituisse un operatore italiano specializzato nella fornitura di servizi cloud alla PA centrale, il terzo tema segnalato dal gruppo di lavoro riguarda le condizioni di gara per la selezione del partner privato (meglio se più di uno). La raccomandazione del gruppo di lavoro è che la gara per selezionare i partner avvenga nel rispetto delle norme a tutela della concorrenza: non può esservi esclusione di partecipanti sulla base della loro nazionalità, delle loro dimensioni, dei modelli di business o di altre caratteristiche, mentre è del tutto opportuno che siano garantiti standard di prestazione, di sicurezza, di interoperabilità e di tutela dell'ambiente in linea con i principi e l'esperienza europea. Più in generale, anche per il nuovo eventuale soggetto si dovranno applicare le norme comunitarie in materia di cloud ed industria dei dati, tenendo conto delle proposte di regolazione attualmente in discussione (Digital Services Act, Digital Markets Act, Data Governance Act), nonché del quadro di regole che verrà definito da Gaia-X.*

*Natura, finalità e prospettive di Gaia-X, ora che da progetto franco-europeo è divenuto un progetto di dimensione europea, costituiscono il quarto tema affrontato dal gruppo di studio. Al riguardo, si sono prospettati tre possibili modelli di riferimento: un modello GSM like, finalizzato alla definizione delle regole "tecniche" (privacy, sicurezza, inter-operabilità, tutela ambientale); un modello Airbus like, che prevede invece un intervento di carattere industriale, nella forma di investimenti diretti da*

*parte pubblica; una “terza via”, definita “ibrida”, in cui - oltre alle regole – si immagina anche una funzione di standardizzazione e brokeraggio verso i servizi di mercato. Peraltro, esaminando i più recenti lavori dell’Associazione, si è evidenziata una quarta possibilità, che potrebbe essere considerata una diversa versione del modello “ibrido”. Si è infatti osservato che – accanto al “prevalente” mandato ad occuparsi del quadro delle regole e degli standard - si sta delineando anche un intervento per la promozione di un layer logico posto al di sopra delle infrastrutture cloud già esistenti. Come si desume dalle posizioni espresse da autorevoli rappresentanti dell’Associazione, oltre alla definizione delle regole, il progetto Gaia-X si dovrebbe occupare anche di un profilo industriale: ossia, l’elaborazione di componenti software che dovranno essere adottate ed implementate da chiunque vorrà offrire servizi conformi al modello proposto nell’ambito dell’iniziativa Gaia-X.*

*Al fine di stimolare un dibattito aperto e non ideologico, tra i policy makers e gli operatori del settore, il gruppo di lavoro presenta tutte e tre le ipotesi, ma, al contempo, dichiara la preferenza pressoché unanime dei suoi partecipanti per l’opzione GSM like – eventualmente integrata da funzioni di coordinamento - e la profonda diffidenza per una soluzione Airbus like.*

*Da ultimo, come raccomandazione generale, il gruppo di lavoro invita a tenere conto delle esperienze maturate in passato, sia in altri paesi (esperienza del “campione nazionale” francese del cloud), sia nel nostro Paese.*

*In particolare, nell’ambito della strategia cloud che il nuovo Ministro per l’Innovazione e la Transizione Digitale dovrà definire, diventa fondamentale tenere conto anche della sinergia tra la struttura abilitante ed il ruolo della Pubblica amministrazione nei processi di digitalizzazione, come verranno indicati nel PNRR (Piano Nazionale di Ripresa e Resilienza).*

*A questo riguardo, si deve ricordare come l’azione di governo, sia a livello centrale che locale, è stata spesso centrata, anche recentemente, sulle nuove tecnologie da adottare e sullo sviluppo e sulla fornitura di servizi di front-end (portali, app, sistemi di pagamento, identità digitale) e non anche sul tema della reingegnerizzazione e della revisione dei processi e dei prodotti della PA<sup>1</sup>.*

*Un cambio di prospettiva di questo tipo creerebbe le condizioni per rendere finalmente possibile una comunicazione diretta tra amministrazioni e, dal punto di vista informatico, la piena interoperabilità dei back-end, il consolidamento delle basi di dati*

---

<sup>1</sup> Si tratta di temi (in particolare la distinzione tra front-end e back-end e il bisogno di far interoperare i back-end delle PA per sviluppare front-end veramente utili) già presenti nel Piano d’azione per l’e-governement elaborato nel 1999 dal prof. Alessandro Osnaghi su mandato del Ministro per la Funzione Pubblica Franco Bassanini e presentato nel 2000.

*del Paese, la razionalizzazione del parco applicativi, premessa quest'ultima indispensabile anche per il passaggio al cloud e l'ottimizzazione dei centri di calcolo e dei sistemi di elaborazione delle amministrazioni. In questa ottica, come già richiamato in precedenza, il pubblico dovrebbe sempre più concentrarsi sulla gestione degli asset strategici del Paese (base di dati e sistemi di back-end), lasciando spazio ai privati per quanto riguarda l'erogazione dei servizi di front-end. Nelle circostanze – assai particolari - in cui, invece, lo Stato decida di operare sul mercato con una propria offerta, si dovrà necessariamente confrontare con le condizioni del mercato, nel rispetto della regolazione vigente e delle norme antitrust.*

## **Premessa**

L'iniziativa Gaia-X, promossa dai Governi di Francia e Germania nel giugno 2020, con la iniziale partecipazione di 22 imprese dei due paesi (11 dalla Germania e 11 dalla Francia), ha assunto una dimensione più solida nel settembre 2020 con la costituzione, da parte dei soci fondatori, di una associazione internazionale senza scopo di lucro di diritto belga, Gaia-X AISBL (dal francese: *association internationale sans but lucratif*).

Di grande importanza il sostegno all'iniziativa venuto dalla Dichiarazione congiunta di 25 paesi membri ad ottobre 2020<sup>2</sup>. In tal modo, l'iniziativa ha assunto una dimensione europea ed al tempo stesso istituzionale.

Nel frattempo, Gaia-X AISBL ha progressivamente acquisito l'adesione di imprese e istituzioni degli altri paesi europei, registrando diverse centinaia di richieste di partnership.

In questo contesto, l'Italia – ossia singole imprese ed alcune associazioni di settore – hanno rivelato un grande interesse, candidandosi a svolgere un ruolo da protagonista.

Per fare cosa? Questa domanda può apparire superflua, alla luce dei documenti programmatici dell'Associazione Gaia-X, consultabili sul relativo sito.

Invece, a nostro avviso, almeno nella fase iniziale ed in modo più attenuato ancora oggi, si è registrata un'ambiguità di fondo su quali siano gli obiettivi dell'iniziativa. Che possono essere semplificati con l'indicazione di due percorsi.

Il primo, di natura regolamentare, riguarda la definizione di un quadro di regole – tecniche e “giuridiche” – per garantire che la fornitura di servizi cloud, da parte di

---

<sup>2</sup> Joint declaration, Building the next generation cloud for business and the public sector in the EU, 15 October 2020.

qualsiasi operatore, avvenga nel rispetto delle norme europee in materia di privacy, tutela dei dati personali, sicurezza, tutela dell'ambiente. Insomma, l'Europa che promuove una regolazione adeguata, sia di natura tecnica, con riguardo agli standard, come avvenuto per il GSM nel caso della telefonia mobile, sia di natura “giuridico-economica”. Sotto questo ultimo profilo, gli esempi più recenti riguardano: il Regolamento Generale sulla Protezione dei Dati (2016), la disciplina del diritto d'autore online (2019), le Direttive sulla regolazione delle comunicazioni elettroniche e dei servizi audio-visivi (2018) ed il recente pacchetto di proposte di regolazione in materia di dati e piattaforme (fine 2020; si veda oltre, paragrafo 2.2) e di Intelligenza Artificiale (aprile 2021).

A tale riguardo, è stata coniata l'espressione *Brussels effect*, ad indicare la capacità dell'Europa di definire un quadro di regole che diviene riferimento per altri paesi, occidentali in primo luogo<sup>3</sup>.

Il secondo percorso è invece meno evidente, mai esplicitamente indicato, almeno nell'ambito dei lavori di Gaia-X: l'idea di costituire un campione europeo nel mercato del cloud, per contrastare l'indubbia egemonia dei grandi operatori statunitensi (Amazon, Microsoft, Google, innanzitutto) e l'avvento di quelli cinesi (Alibaba).

In questo caso, si è evocato il “modello Airbus”, ossia una sfida portata sul piano industriale, per giustapporlo al “modello GSM” o – più in generale – alla strategia fondata sulla definizione di regole coerenti con il rispetto dei valori fondamentali su cui si basa l'Unione europea.

In questo *policy brief*, si esamineranno entrambe le prospettive, ed alcune possibili alternative.

Ai capitoli 1 e 2 è affidato l'esame della regolazione.

In particolare, il primo capitolo richiama alcuni aspetti tecnici dei sistemi di Cloud Computing, illustra i principali servizi e modelli di cloud attualmente disponibili sul mercato, ed accenna ai profili di sicurezza.

Il secondo capitolo, si occupa della regolazione “giuridico-economica”, con specifica attenzione alla disciplina dei dati, tema connesso ma distinto da quello dell'industria del cloud: proprietà ed accesso, sono essenzialmente gli aspetti considerati. In particolare, verranno esaminati i possibili percorsi per una disciplina dei dati e dei servizi cloud nell'ambito della strumentazione a disposizione dell'Unione Europea.

Il capitolo 3 sarà dedicato ad esaminare le implicazioni di carattere competitivo ed industriale, con una analisi delle iniziative di “politica industriale” in atto od annunciate

---

<sup>3</sup> Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

dall'Unione europea. Una attenzione specifica verrà riservata al progetto di un cloud nazionale per la Pubblica Amministrazione, come inizialmente previsto dal Decreto Semplificazioni<sup>4</sup> ed ora incluso tra i progetti del Piano Nazionale per la Ripresa e la Resilienza (PNRR) presentato dal Governo.

Infine, nel capitolo 4, si svolgeranno alcune considerazioni conclusive, allo stato delle conoscenze e del dibattito, entrambi in forte evoluzione, con riguardo alle prospettive di un “campione europeo” capace di competere con le imprese che dominano l'industria mondiale del cloud, e quali possibilità vi siano di rafforzare il potere contrattuale dei clienti, ossia di imprese e amministrazioni pubbliche che, sempre di più, si orientano verso servizi cloud, rinunciando ad internalizzare attività di raccolta, conservazione, elaborazione dei propri dati.

Alcune prime riflessioni saranno poi destinate ad esaminare le diverse possibili prospettive del progetto Gaia-X, al fine di acquisire punti di vista dei partner della ricerca, per una successiva elaborazione, alla luce delle richiamate evoluzioni sia di Gaia-X, che dell'Alleanza su Cloud e Dati.

## **Capitolo 1. L'industria del cloud: profili infrastrutturali, di mercato e di regolazione “tecnica”**

### **1.1. Cloud Computing e Gaia-X**

Il *Cloud Computing* è un paradigma informatico grazie al quale è possibile offrire l'accesso remoto a risorse *hardware e software* secondo una varietà di modalità ed opzioni volte a soddisfare una pluralità di esigenze facendo leva sulla virtualizzazione e sull'orchestrazione efficiente di risorse utilizzabili, anche in modalità condivisa, ma con adeguate garanzie di sicurezza, privacy e condivisione dei dati<sup>5</sup>.

L'offerta di Cloud Computing si articola per modelli di servizio (*infrastruttura, piattaforma e applicazione*) e modelli di dispiegamento (*pubblico, privato, comunitario ed ibrido*). Più recentemente, avendo assunto particolare rilevanza il luogo

---

<sup>4</sup> Il decreto prevede disposizioni volte a favorire la realizzazione di un cloud nazionale per tutelare l'autonomia tecnologica del Paese, mettere in sicurezza le infrastrutture digitali della Pubblica Amministrazione, garantire la qualità e la sicurezza dei dati e dei servizi digitali.

<sup>5</sup> È importante chiarire in questo contesto la differenza tra infrastruttura cloud e applicazione: il cloud può essere definito come un “contenitore” all'interno del quale vengono inseriti i dati senza però consentire al proprietario dell'infrastruttura cloud di avere accesso a quei dati. Il cloud non gestisce i dati, ospita applicazioni che sono il soggetto che ha accesso ai dati. Si tratta quindi di due mercati distinti.

di collocazione delle risorse elaborative, si è iniziato anche a distinguere fra *Core Cloud* ed *Edge Cloud*. In particolare, il *Core Cloud* centralizza le risorse computazionali in data center di grandi dimensioni, per garantire elevate prestazioni nella elaborazione e nella memorizzazione dei dati, mentre *l'Edge Cloud* distribuisce le risorse in data center collocati in prossimità degli utenti, per garantire basse latenze nella trasmissione di informazioni critiche e migliorare la consegna di grandi volumi di traffico (con conseguente riduzione del traffico in rete).

I servizi *Core Cloud* sono offerti principalmente dai grandi player multinazionali Over The Top (OTT), che in questo ambito sono anche detti *Hyperscaler* (Amazon, Microsoft, Google, etc.), mentre i servizi di *Edge Cloud* sono alla portata degli operatori presenti nei territori ove si trovano gli utenti e che possono valorizzare i propri asset per ospitare *mini-datacenter*.

L'ecosistema cloud federato europeo Gaia-X, invece, attraverso la definizione di interfacce aperte e condivise tra gli attori, consente la creazione di un modello flessibile che mette a disposizione del mercato la possibilità di:

1. accedere ad una pluralità di offerte alternative e gestire il *cambio di provider* e la *portabilità dei dati* con impatti marginali;
2. beneficiare di un *presidio europeo* per il rispetto dei requisiti e delle norme di *sicurezza, privacy e titolarità* nel trattamento dei dati;
3. costruire in maniera semplificata strategie di *multi-cloud ibrido privato e pubblico*, con opportuna calibratura tra *Edge* e *Core Cloud*.

L'approccio federato ha il vantaggio di consentire la crescita dell'intero ecosistema in modo aperto, andando a valorizzare in modo virtuoso gli *asset* specifici degli operatori presenti nel territorio e quelli dei grandi player internazionali.

È essenziale sottolineare che il processo di trasformazione abilitato dal cloud nella sua formulazione più moderna e completa non è un mero trasferimento degli stack elaborativi dalla computer room, o dal datacenter aziendale, ai sistemi in Cloud (secondo quello che viene chiamato "*lift & shift*"), ma prevede una vera e propria revisione dei processi interni ed esterni alle organizzazioni, con una riconfigurazione radicale delle modalità operative, delle catene del valore e spesso dei modelli di business.

La messa a punto di un quadro di riferimento strategico chiaro e la maturazione presso le aziende di una cultura e di competenze in grado di cogliere in modo profondo gli spunti della trasformazione digitale costituiscono un fattore chiave per lo sviluppo dell'economia del Paese.

## 1.2. Cenni agli aspetti tecnici dei sistemi di Cloud Computing

In generale, sono tre le tecnologie alla base del *Cloud Computing*: la *virtualizzazione*, i meccanismi di *multitenancy* e le *architetture orientate ai servizi* (SOA – Service Oriented Architecture).

La componente tecnologica essenziale è data dalla virtualizzazione, ossia dalla possibilità di associare alla parte fisica dell'infrastruttura un ambiente virtuale di calcolo o di altre applicazioni (ad esempio *storage*). La virtualizzazione consiste nel creare versioni virtuali di risorse fisiche, quali ad esempio *server*, spazio di memoria e sistemi di rete, come nel caso del modello di *Infrastructure as a Service*, di cui si parlerà nel seguito.

La virtualizzazione consente di definire dinamicamente le caratteristiche delle risorse virtuali e la loro mappatura sulle risorse reali. Questo permette l'ottimizzazione delle risorse e la capacità di far fronte a variazioni nelle esigenze di utilizzo da parte degli utenti.

La seconda componente è la *multitenancy*. Con questo termine, si fa riferimento ad un principio architeturale in base al quale una singola istanza di un'applicazione installata su di una macchina (del *Cloud Provider*) può essere utilizzata da più utenti (i clienti del servizi *Cloud*), mantenendo separati i dati. Si può quindi attivare una singola istanza del servizio (cioè dell'applicazione *software*) senza dover replicare architetture isolate dedicate.

Con architettura orientata ai servizi si fa riferimento ad una serie di principi di disegno architeturale che abilitano l'integrazione e l'aggiunta di servizi, senza che ciò comporti il ridisegno dell'interna architettura *software*. Il funzionamento è dato dall'interazione di diversi servizi, ciascuno dei quali svolge una micro-funzione (*microservices*).

Tramite un'architettura SOA si possono quindi aggiungere nuovi servizi o aggiornare e modificare le modalità con le quali i servizi vengono erogati o interagiscono tra loro, per rispondere meglio a specifiche esigenze.

Questo risulta molto utile nelle architetture di *cloud computing*, all'interno delle quali si possono “accendere” o “spegnere” servizi in modo relativamente semplice a seconda delle necessità.”

## 1.3. I modelli di servizio

Il *National Institute of Standards and Technology* (NIST), definisce tre i modelli di servizio per il *Cloud Computing*. Si tratta di tre modelli che rappresentano tre diverse alternative offerte ai clienti, in cui viene modulata in maniera differente la responsabilità tra cliente e fornitore di servizio, e quindi la delega al fornitore di

servizio di svolgere compiti di approvvigionamento e di conduzione operativa delle risorse *hardware* e *software* che compongono l'infrastruttura di erogazione dei servizi *cloud*.

Tutti i modelli di servizio e tutti i fornitori offrono interfacce di *configurazione*, *acquisto* e *provisioning* dei servizi basate su portali con interfacce grafiche e guide che consentono di acquistare e pagare *online* i servizi, nonché di svolgere le operazioni di conduzione operativa e monitoraggio delle prestazioni in capo ai clienti (modalità “*self-service*”).

Il modello *Infrastructure as a Service* (IaaS) prevede che il cliente si approvvigioni di servizi infrastrutturali di base quali strutture di elaborazione (*core* equipaggiati con risorse tratte da un catalogo di alternative) e di memorizzazione di massa (anche in questo caso con caratteristiche e dimensioni da catalogo). Normalmente, l'acquisto di queste componenti si accompagna all'acquisto di servizi legati alla rete, utili sia per la realizzazione di connessioni tra le componenti in cloud, ma anche per la comunicazione tra *datacenter* e siti di fruizione del cliente.

Il modello di servizio *Platform as a Service* (PaaS), prevede che il cliente si approvvigioni dal fornitore di servizi a valore aggiunto più elevato rispetto alle infrastrutture di *processing* e *storage*, e più precisamente di ambienti di sviluppo o di strumenti di *middleware* (es, *database*, ERP, CRM, Portali, ...), su cui basare lo sviluppo delle proprie applicazioni, configurando le piattaforme o sviluppando parti di codice proprio. In questo caso la frontiera di responsabilità si sposta ulteriormente verso il fornitore, con vantaggi che si aggiungono a quelli già evidenziati per il modello IaaS, riducendo ulteriormente il carico sistemistico e gli oneri di approvvigionamento in proprio (come investimento) delle piattaforme di sviluppo e del *middleware*. All'area del modello PaaS, che si rivolge agli sviluppatori e quindi non agli utenti finali di un servizio applicativo, sono riconducibili anche il paradigma dello sviluppo (detto *Cloud Native*) di *Container as a Service* (CaaS) e *Function as a Service* (FaaS), che offrono maggiore flessibilità nella modularizzazione delle componenti funzionali trattate.

Il modello *Software as a Service* (SaaS) esternalizza completamente lo *stack* IT, con il cliente che si approvvigiona di un servizio applicativo, tipicamente *standard*, offerto dal *provider*, spostando ulteriormente la linea di responsabilità verso il fornitore e estendendo i benefici anche all'area applicativa ed azzerando completamente gli oneri di programmazione e di conduzione sistemistica e mettendo direttamente a disposizione degli utenti finali i servizi applicativi.

Con il termine *Everything as a Service* (XaaS) si ricomprende la vasta gamma di prodotti, strumenti e tecnologie che stanno emergendo come nuove e popolari offerte

di servizi cloud, ciascuno focalizzato su un ambito e per cui è stato coniato un apposito termine.

Tra i servizi più noti vi sono *Desktop as a Service* (DaaS), *Disaster Recovery as a Service* (DRaaS), *Unified Communications as a Service* (UaaS), *Artificial Intelligence as a Service* (AIaaS), *Blockchain as a Service* (BaaS) e *CRypto as a Service* (CRaaS), e così via.

#### 1.4. Modelli di dispiegamento del cloud

Accanto ai modelli di servizio, il NIST definisce quattro modelli di dispiegamento delle tecnologie di *cloud computing*: pubblico, privato, comunitario e ibrido.

Il modello di *cloud pubblico* prevede la fornitura di servizi informatici pubblici su Internet da parte di un fornitore che investe in risorse di *computing* e le colloca in propri *datacenter* distribuiti.<sup>6</sup> I servizi *cloud* pubblici sono offerti al mercato, a fronte di un compenso basato sull'uso, oppure (anche) gratuitamente. Nel *cloud* pubblico, il fornitore è responsabile della gestione e della manutenzione dei sistemi e dell'ambiente fisico in cui questi ultimi sono dispiegati in modo sicuro.

Il modello di *cloud privato* prevede la fornitura di risorse e servizi informatici ad una singola organizzazione che vi accede tramite Internet o una rete interna privata. Un *cloud privato* può essere gestito internamente all'organizzazione, dotata di proprie infrastrutture e strutture di esercizio, o da un fornitore terzo a cui esternalizza la fornitura di servizi che può avere varie gradazioni. Il *cloud privato* offre molti benefici propri del *cloud pubblico*, compresi *self-service* e scalabilità, ma consente anche un maggiore controllo delle risorse e dei dati e una maggiore personalizzazione dei servizi. Queste prerogative sono legate all'obiettivo di realizzare e governare direttamente livelli di sicurezza e privacy.

Il cloud comunitario, o *Community Cloud*, è un modello di implementazione basato su un'infrastruttura condivisa da diverse organizzazioni che si sono accordate per una forma di condivisione tra soggetti conosciuti (che costituiscono la *Community*) con l'obiettivo di realizzare una forma di condivisione ristretta e più controllata.

Si realizza un *cloud ibrido* quando i servizi informatici vengono organizzati combinando implementazioni cloud di tipo pubblico e privato, con una distribuzione dei *workload* che mappa in modo mirato le due modalità in relazione al bilancio

---

<sup>6</sup> I servizi di cloud pubblico possono essere anche erogati tramite connessioni private e non sulla rete internet pubblica. Ciò che rileva ai fini della definizione di cloud pubblico è che le infrastrutture di cloud non sono dedicate ad un singolo cliente, ma condivise fra più clienti e quindi, come tali, "pubbliche".

requisiti/costi dei diversi ambiti di automazione. In questo scenario, estremamente diffuso e comunque presente in fase di progressiva adozione del *cloud*, debbono essere messi in atto adeguati meccanismi per gestire le partizioni dei sistemi nei due ambiti e le eventuali relazioni o esigenze di inter-lavoro.

Il concetto di *multi-cloud*, ossia il ricorso da parte di una singola organizzazione ai servizi di più *cloud provider*, è un concetto che si sta diffondendo rapidamente nel mercato con la duplice finalità di adottare le soluzioni proposte dai diversi fornitori di servizi più rispondenti alle proprie esigenze e di ridurre la dipendenza da un unico provider. Chiaramente, l'opzione *multi-cloud* si può combinare con le modalità ibride (determinando un assetto di tipo “*multi-cloud ibrido*”).

Il numero e la dimensione dei carichi di lavoro informatici è in costante crescita e, con essi, anche l'esigenza del mercato di contare su una struttura cloud il più possibile flessibile, che si adatti a workload consolidati e ad applicazioni cloud native. L'approccio *multi-cloud* può quindi essere la strategia più adatta a questo tipo di esigenza. Gartner prevedeva che nel 2020 il 75% delle aziende che usano servizi IaaS su infrastrutture cloud adotterà una strategia *multi-cloud*. Previsione che, stando ai report di Flexera, di cui si parlerà nel seguito, è risultata corretta.

Il termine *multi-cloud* negli ultimi anni ha avuto due accezioni. La prima relativa agli utilizzatori che si servono di diverse infrastrutture Cloud sia per la parte IaaS che per le parti PaaS e SaaS: si tratta tipicamente di aziende che utilizzano un cloud provider per la parte puramente infrastrutturale delle proprie piattaforme IT e che si avvalgono, per alcune tipologie di software aziendali (per esempio CRM online come Salesforce, Dynamics 365, ERP online o strumenti di collaboration come Office 365 o Google Suite) di soluzioni SaaS o PaaS. La seconda accezione è invece legata alla esigenza di espandere il tema dell'hybrid cloud infrastructure su più public cloud provider. Si tratta del modello multi-cloud infrastrutturale che dovrebbe permettere alle aziende di usufruire della parte IaaS su più piattaforme cloud, sia private, sia pubbliche, integrando anche le risorse di Edge computing. Un esempio tipico è quello di un'azienda che vuole utilizzare macchine virtuali o container su più piattaforme andando a selezionare sul singolo cloud provider le soluzioni che più gli convengono sia in un'ottica di performance, sia in un'ottica di efficienza economica.<sup>7</sup> Il tutto orchestrato da una singola piattaforma di erogazione. Guardando al mercato del multi-cloud infrastrutturale sono ancora poche le soluzioni in grado di gestire questi livelli di complessità.

Il primo Hyperscaler che si è lanciato su questa tipologia di servizio è Google Cloud

---

<sup>7</sup> Usando per esempio S3 di Amazon combinando la parte di ECS - macchine virtuali - su più cloud come quelli di Azure e AWS stesso.

con Anthos poco meno di due anni fa. Di fatto la piattaforma Anthos è in grado di gestire più tipi di workload, in più ambienti (AWS di Amazon, Azure di Microsoft, e Google Cloud di Alphabet), in più località (regions)<sup>8</sup>.

Il secondo caso è quello proposto da Microsoft con Azure, Arc. Attraverso un unico pannello di controllo, i clienti possono gestire le risorse di Azure attraverso più cloud. Questo significa che tutte le innovazioni di Azure sono tecnicamente disponibili ovunque, indipendentemente dal fatto che si trovino su cloud o addirittura in sede.<sup>9</sup>

Anche AWS con la piattaforma Outposts risponde alle esigenze dei clienti che vogliono avvalersi di architetture cloud ibride. Il servizio consente ai clienti di utilizzare i servizi di elaborazione e archiviazione AWS quali Virtual Machine e Storage all'interno dei propri data center, ma con hardware fornito da AWS in combinazione con le risorse del cloud Pubblico.

Google Cloud, Anthos e Microsoft Azure Arc hanno approcci tecnici abbastanza simili; entrambi sfruttano Kubernetes e i *container* per fornire soluzioni complete: on-premise, nella propria piattaforma cloud pubblica o nel cloud di un concorrente.

AWS Outposts, d'altra parte, si concentra esclusivamente sui clienti che necessitano di avere soluzioni on-premise combinate alle risorse AWS pubbliche. Inoltre, utilizzando l'hardware fornito da AWS stesso, Outposts tende a semplificare il modello ibrido e salvaguardare l'investimento del cliente grazie all'uso del proprio hardware ingegnerizzato per supportare al meglio il software del cloud di AWS.

---

<sup>8</sup> La soluzione di Anthos è particolarmente focalizzata alle soluzioni di containerizzazione che utilizzano Kubernetes. Anthos, infatti, consente alle organizzazioni di eseguire Kubernetes sia su cloud che on-premise, garantendo una gestione semplificata in termini di installazione, aggiornamento, gestione della configurazione, sicurezza e osservabilità.

<sup>9</sup> Arc supporta anche VM e cluster Kubernetes in esecuzione su altri cloud pubblici come AWS e Google Cloud.

## Differenze nell'offerta Multicloud dei principali Public Cloud Provider

	AWS Outposts	Azure Arc/Stack	Google Anthos
GESTIONE UNIFICATA DELLE RISORSE CLOUD ED ON-PREMISES	■	■	■
SALVATAGGIO DATI SULL'EDGE PER L'ELABORAZIONE LOCALE	■	■	■
GESTIONE DEL DATO CRYPTATO «AT-REST» ED «IN-TRANSIT» TRA ON-PREMISES E CLOUD	■	■	■
HARDWARE INSTALLATO E GESTITO DAL CLOUD PROVIDER	■		
ESTENSIONE SERVIZI PUBLICCLOUD ON PREMISES	■	■	
SUPPORTO SERVIZI SERVLESS E WORKLOAD		■	■
SUPPORTO MULTICLOUD		■	■

Esistono anche alcuni cloud provider nazionali che stanno sviluppando tramite orchestratori proprietari e uso di piattaforme open source quali Openstack questo tipo di funzionalità. Ed esempio in Italia, Retelit, si propone come operatore multi-cloud in grado di orchestrare piattaforme IaaS su più ambienti cloud sia privati che Azure e AWS.

Esistono anche realtà private che stanno iniziando ad adottare soluzioni simili appoggiandosi a vendor che offrono soluzioni commerciali in grado di garantire il multi-cloud in ambienti tipicamente di containerizzazione.

Alcuni dei prodotti che potrebbero rientrare in questa categoria sono

- VMware CloudHealth / Tanzu
- Giantswarm
- Rancher
- Embotici
- Flexera

Queste piattaforme, in particolare, si occupano di provisioning, automazione, ottimizzazione dei costi, governance delle politiche e controllo dei costi.

Un'ulteriore spinta sul Multi-cloud viene dalle società di Gaming che tramite l'utilizzo di container e data center geograficamente distribuiti sul territorio in modalità Edge computing sono interessate a utilizzare la modalità multi-cloud per rendere disponibili i container su piattaforme diverse tra loro, ma vicine all'utente finale e quindi in grado di garantire la migliore *user experience* e bassa latenza.

Recentemente, sta crescendo l'interesse per *l'Edge Computing*, ossia la tendenza ad

avvalersi di servizi che fanno uso di risorse, quali capacità di elaborazione o memorizzazione, dispiegate in prossimità dei luoghi in cui i dati sono generati ed utilizzati.<sup>10</sup> Il termine *Edge*, ad indicare il bordo o la periferia della rete, si contrappone al *Core* che prevede la localizzazione delle risorse IT in datacenter remoti e spesso di localizzazione geografica non ben definita e mutevole.

Uno spostamento dal centro alla periferia, dal core verso l'edge, che rappresenta un cambio di paradigma soprattutto per le applicazioni cloud native. Il modello edge computing non vuole solo "spostare" il problema dal centro verso la periferia, ma rendere la gestione della rete e del dato più intelligente. L'applicazione, dunque, può essere sviluppata per gestire i dati che hanno bisogno di poca elaborazione sui nodi periferici e mandare invece sul sistema centrale quelli che hanno bisogno di capacità elaborative elevate.

Proprio sul concetto di prossimità si fonda l'edge computing. Funziona infatti spostando l'archiviazione, la gestione e l'elaborazione dei dati verso i nodi periferici, dove i dati sono generati da applicazioni, dispositivi e utenti, lontano dal cloud centralizzato o dalla rete centrale. I nodi edge possono assumere la forma di piccoli data center, micro-data center in shelter così come di singoli dispositivi o sensori.

L'edge computing può essere applicato in modo vantaggioso ovunque la larghezza di banda, la bassa latenza o la gestione localizzata di grandi volumi di dati, siano elementi decisivi e critici per la fornitura di servizi di alta qualità.

Nell'ambito della distribuzione di contenuti e di *network optimization* vediamo come l'applicazione nell'edge di soluzioni come il Content/DNS Caching migliorano di fatto la user experience ("*QoE Improving*") del cliente e ottimizzano i costi di trasporto e la gestione del traffico dati negli operatori. Soluzioni di *Performance Optimization* quali Protocol Accelerators e breakout session, invece, sono in grado di ottimizzare il flusso applicativo TCP andando di fatto a intercettare la chiamata sull'edge in modo da diminuire il delay dovuto alla maggiore latenza verso il core.

Con l'avvento dell'IoT e del 5G gli operatori stanno adottando soluzioni di MEC (Multi-access Edge Computing) per implementare le funzioni di Cloud-Radio Access Network (Cloud-RAN) che consentono di modernizzare la distribuzione delle funzioni di front-haul, mid-haul e back-haul con l'obiettivo di soddisfare i requisiti critici di latenza dei servizi Ultra-Reliable Low Latency (URLLC) e di efficienza nel trattamento dei voluminosi traffici generati dall'Internet of Things quali Massive Machine Type Communications (MMTC) e enhanced Mobile BroadBand (eMBB).

---

<sup>10</sup> Si pensi ai sensori dell'Internet delle Cose che generano dati e che fruiscono dei risultati delle funzioni di computing.

La gestione del flusso dati tra il dispositivo, la rete, l'edge e il core, dove risiedono parti dell'applicazione e del dato, diventa critico e quindi di fondamentale importanza diviene la valutazione del tema della sicurezza.

L'edge computing può diventare un abilitatore di fondamentale importanza delle tecnologie blockchain sia a livello di *protocollo* (tra l'utente e l'applicazione), sia a livello di *distributed application* sull'intera catena tra gli edge e il core.

Affinché i nodi blockchain possano comunicare tra loro, i dati devono viaggiare attraverso l'intera rete e tornare indietro, che è il modo in cui scorre il traffico nel cloud computing. Una rete di edge computing creerebbe meccanismi per nuovi flussi di dati, da server a server, eliminando la necessità che i dati debbano attraversare la rete centrale.

Una delle sfide dell'edge computing nel mondo degli operatori telco è quello di creare un modello commerciale che faciliti l'accesso degli sviluppatori all'infrastruttura cloud edge. Esiste il rischio che l'infrastruttura di elaborazione edge rimanga frammentata tra gli operatori di telecomunicazioni, il che significa che uno sviluppatore di applicazioni dovrebbe interfacciarsi con ogni operatore di telecomunicazioni per garantire che l'applicazione funzioni. In caso contrario, lo sviluppatore rischia di non essere in grado di garantire un'esperienza coerente (bassa latenza).

La blockchain potrebbe essere utilizzata per garantire la distribuzione delle applicazioni in maniera sicura tra i vari nodi edge di differenti operatori garantendone la "data sharing" ed insieme al multi-cloud potrebbe creare un mercato decentralizzato di edge computing che combini i fornitori di infrastrutture edge con coloro che lo richiedono.

Soprattutto nelle aree periferiche, lontane dai centri delle grandi città e metropoli, l'edge computing è uno degli esempi più evidenti di come la tecnologia possa essere sfruttata per portare un miglioramento reale, attraverso diverse soluzioni già pronte all'uso.

Uno dei campi di applicazione più interessanti dell'edge computing è il settore sanitario, dove il calcolo decentrato potrebbe aiutare ad accelerare la comunicazione da macchina a macchina e da macchina a persona, fornendo applicazioni e servizi medici e distribuendo i carichi di lavoro in piccoli data center locali. I dispositivi sanitari IoT, se interfacciati con data center periferici, possono estendere l'azione del personale medico anche ai pazienti che si trovano in aree con scarsa connettività.

Anche in ambito smart city, nei centri urbani intelligenti si possono utilizzare i sistemi di calcolo decentrato per generare informazioni in tempo reale sui trend di traffico attraverso dispositivi come telecamere e semafori. Le medesime tecnologie possono

essere utilizzate per creare servizi intelligenti per la gestione del traffico stesso.

Esiste ed esisterà sempre più, infatti, un volume significativo di dati che viene prodotto con sensori IoT in tutti i tipi di endpoint, dai semafori fino ai bidoni della spazzatura. Per queste informazioni l'elaborazione periferica permette il contenimento dei costi, oltre che l'efficienza dei servizi.

Infine, un ulteriore campo di applicazione delle tecnologie di edge computing è il gaming, dove al momento le soluzioni più diffuse sono di tipo centralizzato in cui gli utenti si collegano direttamente ai data center core che elaborano il gioco, con evidenti problemi di latenza. Collegandosi invece localmente alla rete edge, gli utenti sperimenterebbero livelli ridottissimi di latenza. È questo il motivo per il quale le società di gaming stanno iniziando a sperimentare modelli di utilizzo dell'edge computing secondo i quali il cliente utilizza le schede grafiche in cloud rendendo l'elaborazione dei dati sul dispositivo del cliente più snella (e di fatto ampliando l'uso del gaming anche a chi non può permettersi computer con schede grafiche costosissime).

### **1.5. La sicurezza e la resilienza del dato nel Cloud**

Il tema della sicurezza e della resilienza dei dati nel cloud è un tema di assoluta importanza, che deve essere oggetto di attenta valutazione in ogni scelta aziendale che riguarda i servizi cloud e che deve affrontato secondo le consuete categorie (almeno nell'ambito della sicurezza informatica) della sicurezza fisica e della sicurezza virtuale ai vari livelli dell'infrastruttura.

Circa la sicurezza fisica e la robustezza delle infrastrutture è necessario assicurarsi che i Data Center e le piattaforme Cloud dove vengono ospitati i dati garantiscano il massimo grado di affidabilità sia in termini di livelli di servizio, sia in termini di sicurezza fisica e virtuale negli accessi. In merito al primo punto, bisogna garantire la ridondanza delle connessioni di rete e quella delle infrastrutture di erogazione di energia. Entrambe devono poter far fronte a guasti multipli, garantendo comunque la salvaguardia dei dati e nei casi più critici lo spegnimento in sicurezza dei server evitando la corruzione dei dati. Bisogna in aggiunta verificare che i Data Center abbiano adeguati sistemi di prevenzione degli incendi e di controllo della temperatura e dell'umidità. Nel caso in cui vengano garantiti servizi di *Disaster recovery* e *Business Continuity*, è fondamentale che la distanza fisica tra le infrastrutture garantisca la corretta funzionalità dei servizi. Ad esempio, per garantire il *Disaster Recovery* vi dovrebbero essere almeno 100 chilometri di distanza tra i Data Center che forniscono il servizio, mentre per la *Business Continuity* bisogna garantire tempi di latenza di pochi millisecondi, parametro che varia in base alle applicazioni che devono essere

gestite.

Ai fini della sicurezza è poi di estrema importanza la disponibilità di un sistema di backup che faccia uso di:

- 1) tecnologie per il backup diverse da quelle utilizzate per i dischi di produzione, al fine di evitare che in caso di malfunzionamenti software o hardware il danno si propaghi anche ai sistemi di backup;
- 2) crittografia del dato sia durante il suo trasferimento, sia nella fase di storage su altro dispositivo;
- 3) un sistema di backup che garantisca diversi gradi di copia e *retention* del dato. (Regola del 3-2-1);
- 4) modalità di salvataggio dei dati di backup su dischi ed in locali diversi da quelli in cui risiede il dato di produzione ed che garantisca che almeno una delle copie risieda in un Data Center diverso da quello di produzione;
- 5) un sistema di monitoraggio che garantisca la corretta esecuzione del backup e che i dati del backup non siano corrotti.

Gli ultimi eventi di cronaca nel mondo Cloud ci fanno capire come spesso queste misure di prevenzione che sembrano banalità, spesso vengano sottovalutate o applicate solo in parte da chi eroga servizi Cloud.

Sempre in tema di sicurezza fisica e virtuale degli accessi è importante garantire che i Data Center abbiano un presidio o un monitoraggio da remoto H24 che permetta il controllo degli accessi alle infrastrutture ed alle aree private (*cage*) dedicati ai dati. Gli accessi a tali infrastrutture devono essere normati e garantiti solo a personale autorizzato ad eseguire determinati lavori.

All'interno delle infrastrutture Cloud, esistono diversi sistemi di sicurezza in grado di garantire la protezione degli ambienti virtuali. A titolo di esempio vi sono soluzioni che si occupano degli accessi alle piattaforme tramite appositi sistemi di Key Access Management, Identity Access Management e Controllo degli accessi.

Le soluzioni più utilizzate per garantire la sicurezza perimetrale, come Firewall e Protezioni Antivirus e Anti-Spam sono ormai uno standard nelle infrastrutture Cloud. Tuttavia, va verificata attentamente l'offerta e l'implementazione di questi sistemi con appositi meccanismi di controllo, di correlazione e di *log management* che garantiscano l'efficacia nella prevenzione degli attacchi.

Infine, vista la loro frequenza non si possono sottovalutare i cosiddetti Distributed Denial of Service (DDoS). Sono questi gli attacchi più frequentemente utilizzati per

danneggiare le aziende ed il loro business e che vengono esercitati saturando le connessioni dei server con quantitativi di traffico internet anomalo, al fine di congestionare la piattaforma e non permettere agli utilizzatori di accedere correttamente ad esse. A tal fine, le piattaforme Cloud devono adottare sistemi di mitigazione degli attacchi DDoS quali scrubbing center e strumenti di *detection* e pulizia.

Al fine di slegare alcune funzioni di gestione della sicurezza relative all'accesso dalla responsabilità del provider di servizi *cloud*, sono nati *player* specializzati: i *Cloud Security Access Broker* (CSAB), secondo la definizione del NIST. I CSAB utilizzano strumenti che possono essere dispiegati in *cloud* o nei siti privati, offrono servizi che si interpongono tra i clienti ed i fornitori di servizi con l'obiettivo di offrire un supporto terzo ed indipendente dal *cloud provider* per mettere in atto le politiche di sicurezza del cliente, utilizzando meccanismi e controlli basati sull'analisi dei rischi applicati ai dati che vengono memorizzati e trattati in *cloud*. I servizi offerti dai CSAB sono nati proprio per colmare alcune lacune in termini di visibilità, conformità, sicurezza dei dati e protezione dalle minacce per i servizi basati su *cloud*. La terzietà del fornitore CSAB rispetto ai *cloud provider* offre garanzie rispetto a possibili rischi di abusi da parte degli addetti che hanno la responsabilità della conduzione operativa dei sistemi presso i *cloud provider* (realizzando una separazione dei compiti specifici di gestione delle misure di sicurezza, quali la gestione degli accessi, delle credenziali e delle chiavi di cifratura).

## **Capitolo 2. La regolazione “giuridico-economica” del cloud: il tema dei dati**

### **2.1. La via “tradizionale” della regolazione dei mercati**

Qualora si volesse affrontare la questione di una disciplina dei dati, con specifico riguardo al tema dell'accesso, una prima ipotesi da considerare riguarda l'inserimento del mercato del cloud e/o quello dei dati nella lista dei mercati di comunicazione elettronica sottoposti a regolazione *ex ante* da parte della Commissione europea. Ovviamente, in via preliminare, sarebbe necessario dimostrare la riconducibilità di questi due mercati ad un più ampio perimetro delle comunicazioni elettroniche: tema impegnativo, che non si intende tuttavia affrontare in questa sede, anche per via delle conclusioni cui si perviene riguardo alla praticabilità di questo percorso.

La lista dei mercati rilevanti suscettibili di regolazione *ex ante* è stata più volte aggiornata dalla Commissione europea, mediante apposite Raccomandazioni: si è così passati dai diciotto mercati individuati inizialmente nel 2003 a soltanto quattro mercati, ossia quelli attualmente regolati, mentre il prossimo passaggio è la riduzione ad un solo

mercato da sottoporre a regolazione ex ante (la rete di accesso fissa di telecomunicazioni). Il modo di procedere della Commissione è stato per progressive eliminazioni, con qualche affinamento nella definizione degli stessi mercati, a testimoniare l'efficacia dell'impostazione seguita per la regolazione dei mercati delle comunicazioni elettroniche. In estrema sintesi, oltre i  $\frac{3}{4}$  dei mercati inizialmente individuati sono divenuti via via concorrenziali, ed affidati quindi alla vigilanza delle autorità di concorrenza, non essendovi più motivi per una regolazione ex ante.

Tanto premesso, appare altamente improbabile che la Commissione proceda in questa direzione, ossia ad integrare la lista attualmente vigente. Ciò per due ordini di ragioni.

In primo luogo, come accennato, la strategia seguita dalla Commissione fin dall'inizio è di ridurre, fino ad azzerare possibilmente, la lista di mercati sottoposti a regolazione ex ante, non prevedendo quindi eventuali integrazioni. In tal senso, si rammenta che – in passato – in occasione delle revisioni della suddetta lista, erano pervenute da alcuni *stakeholders* indicazioni per ampliare l'elenco a nuovi servizi, fundamentalmente con riferimento a quelli offerti dalle piattaforme digitali: in nome di un effettivo *level playing field* tra gli operatori dei mercati delle comunicazioni elettroniche e le grandi piattaforme Internet (denominati anche Over The Top, OTT), si proponeva – soprattutto – di sottoporre gli OTT alle stesse regole in capo agli imprese di telecomunicazioni, ma alcuni suggerivano anche di considerare servizi quali i motori di ricerca, la distribuzione di contenuti digitali e di software, i social network ed il commercio elettronico alla stregua dei mercati di comunicazione elettronica. La Commissione europea non ha mai dato seguito a queste richieste, nel senso che non ha mai veramente considerato la possibilità di estendere la lista dei mercati rilevanti a prodotti/servizi Internet.

In secondo luogo, anche qualora dovesse rivedere l'impostazione fin qui seguita, per inserire nella lista il mercato del cloud e quello – più complesso – dei dati, la Commissione dovrebbe condurre preliminarmente il test dei tre criteri<sup>11</sup>, necessario a concludere che soltanto una regolazione ex ante potrebbe portare a soluzione le problematiche concorrenziali e di tutela del consumatore (eventualmente) riscontrate.

Ora, per quanto riguarda il mercato del cloud, definito in prima battuta come un unico aggregato, senza quindi procedere alla necessaria articolazione in distinti

---

<sup>11</sup> Una chiara esposizione della metodologia per l'applicazione del test dei tre criteri è rappresentata nelle Linee guida del BEREC relative a questo tema. Preliminarmente, il BEREC ricorda che “In line with the 2003 Recommendation, in the new document reference is made to the application of the following three criteria in order to determine whether a market is a candidate market for ex ante regulation: (a) the presence of high and non-transitory barriers to entry; (b) a market structure which does not tend towards effective competition within the relevant time horizon; (c) the insufficiency of competition law alone to adequately address the market failure(s) concerned”.

segmenti/mercati, si osserva sicuramente un ruolo di rilievo di alcuni operatori extraeuropei nelle diverse realtà dei paesi membri; tuttavia, più che una posizione dominante di un soggetto, sembra più plausibile definire un oligopolio ristretto ad un numero limitato di imprese. In relazione alla disciplina degli oligopoli, tuttavia, la Commissione europea non ha finora maturato una posizione altrettanto solida come quella che vi è nei confronti della dominanza di mercato – singola o congiunta.

Queste considerazioni sono ancora più pertinenti nel caso del mercato dei dati, per il quale una articolazione merceologica appare peraltro ancora più opportuna: sono infatti davvero numerose le imprese che, oltre le piattaforme digitali, sono in possesso di quantità straordinarie di dati – personali e non – su cui costruiscono modelli di business e servizi innovativi. Un approccio di tipo settoriale e non generale si presenta come l'unico plausibile. In effetti, in alcuni settori, come ad esempio quello dei pagamenti, opera da alcuni anni una disciplina specifica che prevede l'obbligo di dare accesso alle informazioni detenute dagli istituti di credito, con la finalità di promuovere l'innovazione e la competizione nei mercati dei servizi di pagamento e – più in generale – del mercato creditizio<sup>12</sup>.

In conclusione, alla luce della strategia fin qui seguita dalla Commissione europea di ridurre il perimetro dei mercati di comunicazione elettronica sottoposti a regolazione ex ante, nonché considerando gli assetti di mercato che – *prima facie* – sembrano escludere l'esistenza di posizioni dominanti singole o congiunte nel mercato del cloud ed in quello dei dati, almeno se considerati come macro-aggregati, appare del tutto improbabile che – anche in prospettiva – i mercati del cloud e dei dati – o loro articolazioni – siano inseriti nella lista dei mercati di comunicazione elettronica suscettibili di regolazione ex ante.

In effetti, la Commissione europea – per motivazioni di concorrenza e tutela del consumatore, ma anche di competitività - sta definendo una strategia diversa e più articolata per intervenire sui mercati del cloud e dei dati. Le leve utilizzate sono due: una di natura regolamentare, ma con un approccio diverso dalla regolazione dei mercati delle comunicazioni elettroniche; l'altra di profilo industriale, volta a rafforzare l'industria europea.

Con riguardo a questa ultima, svolgeremo alcune considerazioni nel capitolo 3, mentre di seguito si dà conto delle recenti iniziative comunitarie di tipo regolamentare.

---

<sup>12</sup> Si tratta della Direttiva denominata PSD2: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

## 2.2. La regolazione dei servizi e dei mercati digitali

Più precisamente, sotto il primo profilo, la Commissione ha appena pubblicato tre proposte di regolamentazione dei servizi e dei mercati digitali, con impatto significativo sul mercato dei dati, e – di riflesso – su quello dei servizi cloud.

La proposta di regolamento in materia di servizi digitali, cosiddetto Digital Services Act<sup>13</sup>, riguarda tutti gli operatori a prescindere dalle loro dimensioni ed è sostanzialmente finalizzata a:

- i. assicurare una maggiore sicurezza online, così da aumentare la fiducia degli utenti;
- ii. chiarire le responsabilità collegate alla fornitura di servizi digitali da parte degli intermediari digitali (in particolare le piattaforme online);
- iii. ridurre la frammentazione normativa riscontrabile nei mercati dei paesi membri;
- iv. garantire maggiore trasparenza nell'operato delle piattaforme digitali, in particolare con riguardo al modo in cui usano i propri algoritmi;
- v. realizzare una “parità di trattamento regolamentare” tra servizi offline ed equivalenti servizi on line;
- vi. contrastare usi illegali, o comunque dannosi, dei servizi digitali.

La proposta di regolamento in materia di mercati digitali, cosiddetto Digital Markets Act<sup>14</sup>, complementare al DSA, è innanzitutto volta a rafforzare l'antitrust europeo di fronte al potere di mercato acquisito dalle piattaforme digitali di grandi dimensioni (definiti *gatekeepers*<sup>15</sup>).

Il rafforzamento della strumentazione antitrust viene peraltro accompagnato dalla previsione di una regolazione ex ante, limitatamente ai soli soggetti designati come *gatekeepers*. I principali obblighi in capo a queste imprese riguardano:

- i) l'uso dei dati, per via della enorme quantità di dati raccolti e detenuti, con vincoli severi al loro utilizzo quando ciò può determinare distorsioni concorrenziali nei mercati a valle;

---

<sup>13</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Brussels, 15.12.2020, COM (2020) 825 final.

<sup>14</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), Brussels, 15.1.2020, COM(2020)842 final.

<sup>15</sup> Al fine di individuare questi soggetti, la Commissione propone un set di criteri che riguardano le loro dimensioni, il loro ruolo e la “persistenza” nel tempo del loro potere di mercato.

ii) l'interoperabilità, con l'obbligo di fornirla ai concorrenti ogni qualvolta un *gatekeeper* offre un servizio in un mercato differente (esempio, nel caso di un servizio di pagamento);

iii) la funzione di *self-preferencing*, ossia l'obbligo per il *gatekeeper* di modificare il proprio algoritmo di ricerca per eliminare la pratica (diffusa) di dare preminenza ai propri servizi rispetto a quelli dei concorrenti.

La terza proposta legislativa, denominata Data Governance Act<sup>16</sup>, definisce un quadro regolatorio adeguato alla *data governance*, l'*accesso ed il riutilizzo* dei dati (tra imprese, tra imprese e governo, all'interno delle amministrazioni).

Tra le altre cose, di particolare interesse, sono:

- i) l'istituzione della figura dell'intermediario dei dati, con l'obbligo per ogni paese membro di notificare a Bruxelles i soggetti qualificati come tali;
- ii) una legislazione generale per il *data sharing*, oltre quelle già previste o in corso di definizione a livello settoriale;
- iii) l'istituzione di apposite autorità di vigilanza sia a livello comunitario che nazionale.

Per quanto attiene alla prima proposta rilevante, ossia l'istituzione di un intermediario dei dati, sarà opportuno che, nel corso del dibattito con gli *stakeholders* e nel confronto con il Parlamento ed il Consiglio europei, la Commissione consideri la – diversa – rilevanza che questa figura può assumere con riferimento alla tipologia di impresa utilizzatrice dei servizi cloud.

In termini estremamente semplificati, i “grandi clienti” di settori quali l'energia, i trasporti, le telecomunicazioni – per rimanere nell'ambito delle industrie a rete – hanno ormai maturato una significativa esperienza nelle relazioni con gli *hyperscaler*, mentre, di certo, per il tessuto di piccole e medie imprese che caratterizza l'economia italiana questo intermediario potrebbe assumere un significato importante, riducendo l'asimmetria informativa di cui soffrono ed accrescendo la capacità di contrattazione. In ogni caso, come si dirà anche nel capitolo 4, anche per le imprese di maggiori dimensioni con una già ben avviata transizione al cloud, potrebbero essere utili forme di cooperazione, con lo scambio di *best practices*, ed il rafforzamento della propria forza contrattuale così da bilanciare quello degli *hyperscaler* (*countervailing buyer power*).

Con questo pacchetto legislativo, la Commissione europea ha dato seguito all'iniziativa promossa nel febbraio 2020, con cui veniva aggiornata (ridefinita, in realtà) la strategia

---

<sup>16</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), Brussels, 25.11.2020, COM(2020)767 final.

europea per il digitale, con il programma “Shaping Europe’s Digital Future”.

La nuova strategia veniva descritta come un processo a stadi, di cui venivano immediatamente promossi i primi due passaggi: i) la Comunicazione «*A European strategy for data*», sottoposta a consultazione pubblica; ii) il Libro bianco sull’Intelligenza artificiale («*A European approach to excellence and trust*»).

Inoltre, la Commissione si impegnava a presentare entro dicembre un Digital Service Act, che – nel corso dell’anno – ha assunto una fisionomia diversa, più ampia, rispetto a quella delineata inizialmente, per pervenire alle tre proposte di regolamento appena illustrate.

La diversa articolazione del programma della Commissione trova ragione anche nella necessità di tenere in considerazione le parallele iniziative di altri paesi occidentali, volte comunque a fronteggiare il potere assunto dalle grandi piattaforme online. In particolare, si sono moltiplicate le istruttorie nei confronti dei Big Tech negli Stati Uniti, mentre il Regno Unito è pervenuto ad una proposta di disciplina, con qualche giorno di anticipo rispetto alla Commissione europea<sup>17</sup>.

A questo punto, si può sostenere che la disciplina dei mercati digitali, con particolare riguardo ai mercati dei dati – e dei collegati mercati dei servizi cloud – è affidata alle sorti delle tre proposte di regolamento che ora affronteranno la (lunga) procedura del triloquio, per pervenire, plausibilmente entro un biennio, alla loro approvazione definitiva, a valle di un dibattito che si annuncia assai vivace.

Tuttavia, data la rilevanza del tema e la contemporanea continua azione delle autorità antitrust, sia a livello sovranazionale che nazionale, nei confronti delle grandi piattaforme digitali, è plausibile che i singoli paesi membri dell’Unione europea, anche sulla scorta dell’esempio inglese<sup>18</sup>, intraprendano autonomi percorsi di riforma della disciplina antitrust, con l’attribuzione di competenze di carattere regolamentare alle rispettive autorità di concorrenza. Questa è la strada che, ad esempio, ha scelto la Germania, dove si sta discutendo di emendare la normativa antitrust, assegnando competenze regolamentari al *Bundeskartellamt*.

A questo punto, qualora altri paesi membri decidessero di anticipare il percorso europeo con iniziative nazionali, vi sarebbe il rischio di trovarsi di fronte ad una ulteriore frammentazione del quadro di regole per i mercati digitali, ossia di contraddire

<sup>17</sup> Competition & Markets Authority, A new pro-competition regime for digital markets, December 2020.

<sup>18</sup> Nel Regno Unito, il Governo ha richiesto all’autorità Antitrust (Competition and Markets Authority, CMA) di predisporre un rapporto per definire un nuovo quadro pro-concorrenziale per i mercati digitali. Il CMA, coordinandosi con le autorità per la privacy e di regolazione (Ofcom), ha presentato una proposta, che è stata discussa ad Astrid, nel corso di un seminario introdotto dal CEO di CMA.

la finalità di fondo del nuovo pacchetto legislativo della Commissione europea: la promozione di un *level playing field* unitario, per offrire a utenti ed imprese un contesto di regole chiaro ed efficace.

### Capitolo 3. L'assetto competitivo del mercato europeo del cloud: possibili evoluzioni

#### 3.1. Un quadro generale

Il tema dei dati e dei servizi cloud non è solo oggetto di intervento regolamentare. In modo meno organico rispetto all'impostazione regolamentare, la Commissione europea sta promuovendo iniziative per sostenere l'offerta di servizi cloud e lo sviluppo di un mercato dei dati che sia in grado di promuovere la competitività dell'industria europea e l'efficienza della pubblica amministrazione.

Senza pretese di esaustività, ma solo con l'intento di una prima ricognizione di interventi che possono essere ricondotti nell'ambito di una strategia di politica industriale europea in materia di servizi dati e cloud, si ricordano:

- i. la European Cloud initiative del 2016<sup>19</sup>, volta a rafforzare la posizione dell'Europa nell'ambito dell'innovazione incentrata sull'uso e lo sfruttamento dei dati (principalmente di tipo scientifico) e a promuovere il Digital Single Market;
- ii. il sostegno allo sviluppo di sistemi tecnologici e delle infrastrutture di prossima generazione, anche contribuendo con investimenti nei progetti di elevato impatto (*European High Impact Projects*), per costruire uno spazio europeo dei dati ed infrastrutture cloud affidabili ed efficienti dal punto di vista energetico;
- iii. la volontà dell'Unione europea di potenziare ulteriormente lo scambio transfrontaliero dei dati e promuovere l'economia dei dati tramite l'adozione di un quadro di regole applicabili alla libera circolazione dei dati non personali nell'Unione europea<sup>20</sup>;
- iv. l'avvio di iniziative settoriali per costruire *specifici* spazi europei dei dati, ad esempio con riguardo a: il settore manifatturiero, la salute, la mobilità, il «green

<sup>19</sup> <https://ec.europa.eu/digital-single-market/en/european-cloud-initiative>.

<sup>20</sup> Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (GU L 303 del 28.11.2018, pag. 59); Il principio della libera circolazione dei dati personali è già sancito nel Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

*deal*»;

- v. il già richiamato sostegno alla iniziativa Gaia-X, mediante la citata Joint Declaration;
- vi. la promozione della European Alliance on Industrial Data and Cloud, i cui lavori sono ancora riservati ad un numero ristretto di partecipanti, ma che costituisce, come detto in precedenza, un progetto particolarmente importante, sia per le dimensioni di budget su cui può contare, in quanto legato ad un IPCEI (Important Project of Common European Interest), sia per le relazioni con Gaia-X.

Sul punto iii è da sottolineare l'obiettivo europeo, nell'ambito del regolamento sulla libera circolazione dei dati non personali, di evitare pratiche di "vendor lock-in". La portabilità dei dati tra le imprese, infatti, sta diventando sempre più un elemento determinante in numerose industrie digitali, tra cui i servizi cloud. Con l'articolo 6 del regolamento sulla libera circolazione dei dati non personali, la Commissione si propone quindi l'obiettivo di stimolare l'elaborazione di codici di condotta di autoregolamentazione a livello dell'Unione, nell'ottica di creare le migliori condizioni per lo sviluppo di un'economia dei dati competitiva e fornire all'industria una base per sviluppare codici di autoregolamentazione che disciplinino il cambio di fornitore di servizi e la portabilità dei dati tra i diversi sistemi informatici<sup>21</sup>.

Con riguardo invece alle due ultime iniziative, più direttamente mirate ai dati ed ai servizi cloud, è opportuno rimandare ai testi ufficiali, con riguardo allo specifico tema della promozione dell'industria europea.

In particolare, nella nota "*Towards a next generation cloud for Europe*", la Commissione europea, assieme alla presidenza di turno della Germania, fanno le seguenti affermazioni.

- A common approach to building the European cloud supply will reinforce Europe's digital sovereignty and increase the competitiveness of European business and industry. In parallel, it will support digitalisation for efficient public administrations, better healthcare and a cleaner, more sustainable environment.
- Member States recognise the need for additional investment, enhanced synergies across national initiatives and a coordinated strategy to lead the cloud uptake in the

---

<sup>21</sup> Nel mercato dei servizi cloud, la Commissione ha avviato dei gruppi di lavoro dei portatori di interesse cloud del mercato unico digitale, composti da esperti e utenti professionali cloud. Obiettivo di uno dei sottogruppi è l'elaborazione di codici di autoregolamentazione sulla portabilità dei dati e sul cambio di fornitore di servizi cloud (gruppo di lavoro [SWIPO](#)), mentre un altro sottogruppo sta lavorando allo sviluppo della certificazione di sicurezza dei servizi cloud (gruppo di lavoro [CSPCERT](#)). Il gruppo di lavoro SWIPO si occupa in particolare dello sviluppo di codici di condotta che riguardano l'offerta completa dei servizi cloud: Infrastruttura come servizio (IaaS), Piattaforma come servizio (PaaS) e Software come servizio (SaaS).

private and public sectors across Europe. In particular, as agreed in the Declaration, the Member States' joint actions will focus on:

- i. Combining private, national and EU investment in deploying competitive, green and secure cloud infrastructures and services. This will mean pursuing the next steps together with industry and experts to shape the *European Alliance on Industrial Data and Cloud*.
  - ii. Defining a common European approach on federating cloud capacities, by working towards one set of joint technical solutions and policy norms in order to foster pan-European interoperable EU cloud services.
  - iii. Driving the take-up of more secure, interoperable and energy-efficient data centres and cloud services in particular for small and medium enterprises, start-ups and the public sector.
- A European Alliance on Industrial Data and Cloud will be launched by the end of the year. Within this Alliance, interested Member States, industries and relevant experts will work together to design the detailed business, investment and implementation plan to deploy the next generation cloud capacities for the public and private sector.

L'iniziativa – che il gruppo di lavoro ritiene di grande valenza, anche per le sue relazioni con Gaia-X - è stata poi effettivamente avviata, con lo svolgimento di diversi incontri riservati che si tengono regolarmente da dicembre, finalizzati – almeno per ora - alla redazione delle linee guida sulle *key priorities* dell'Alleanza, con riguardo ad alcune tematiche: energia, edge ed infrastrutture cloud, hardware di prossima generazione, data governance e cybersecurity. All'iniziativa partecipano alcuni rappresentanti di imprese italiane sia del settore telecomunicazioni che del cloud.

Questi sintetici richiami alla nota della Commissione europea sono – ad oggi – l'unica occasione in cui, al di là delle interviste di singoli Commissari europei, viene esplicitata una strategia comunitaria di politica industriale per il cloud, che affianca il percorso di carattere regolamentare.

Rispetto a questo quadro, ancora non del tutto chiaro, nel capitolo 4 si avanzano alcune prime riflessioni sull'evoluzione di Gaia-X e del cloud europeo, per una discussione con i partecipanti al gruppo di ricerca.

### **3.2. Le determinanti dell'adozione dei servizi cloud da parte delle imprese**

Le iniziative menzionate nella sezione precedente nascono tutte dalla consapevolezza della rilevanza del ruolo dei servizi cloud nell'ambito della data economy e della

necessità di dotare l'Europa – riconoscendo un ritardo rispetto agli Stati Uniti ed alla Cina – di una infrastruttura di immagazzinamento e di gestione dati di rilevanza mondiale. Del resto, se dalla Figura 1, che si riferisce ai paesi membri dell'OECD, si evince che a livello aggregato circa il 33% delle imprese con almeno 10 addetti utilizza servizi cloud, andando a vedere le posizioni delle singole nazioni si osserva che solo il 22,5% delle imprese italiane ne fa uso, a fronte del 51,8% degli USA ed il 52,9% del Canada (ma anche del 19,4% della Francia e del 22,4% della Germania).

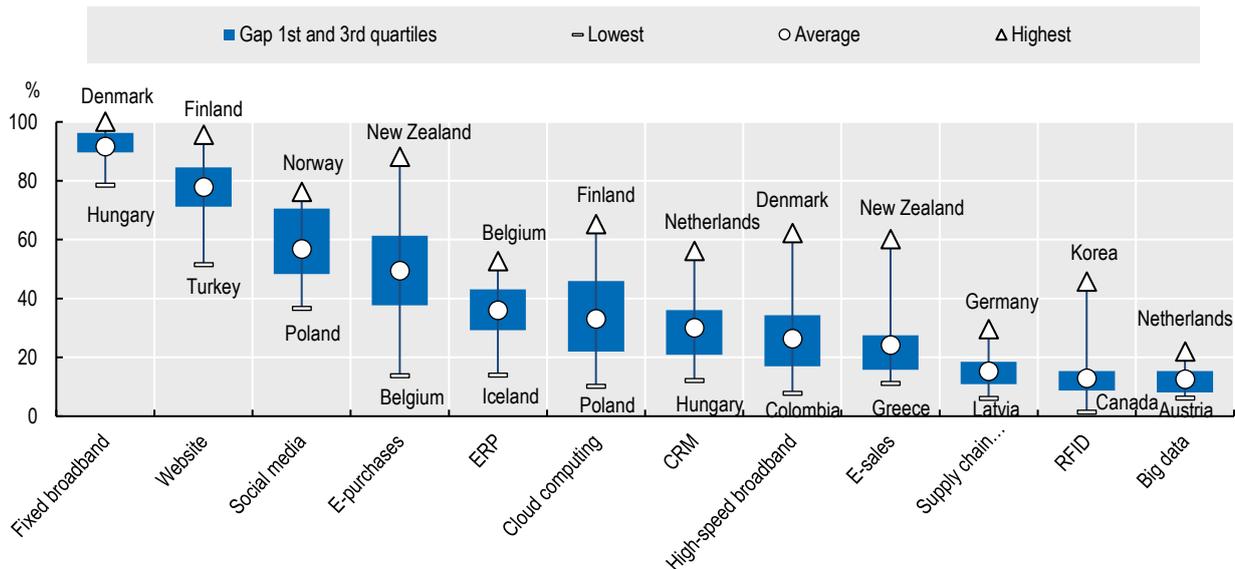


Figura 1 – Diffusione di alcuni strumenti e servizi ICT nelle imprese (come percentuale delle imprese con almeno 10 addetti) 2019. Fonte: OECD Communications Outlook 2020.

Volendo ottenere informazioni sull'utilizzo dei servizi cloud da parte delle imprese italiane con un maggior dettaglio geografico, si può far ricorso al primo censimento permanente delle imprese dell'Istat, relativo all'anno 2018, i cui dati, come è possibile osservare dalla Tabella 1, evidenziano – anche in questo campo – il ritardo delle regioni del Sud rispetto a quelle del Nord. Un ritardo che risulta più marcato di quello relativo all'adozione di software gestionale presso le imprese, e che potrebbe essere spiegato dalla maggiore maturità del mercato dei software gestionali rispetto a quello dei servizi cloud.

Tabella 1 – Utilizzo di software gestionale e servizi cloud nelle imprese italiane con almeno 10 addetti, 2018. Fonte: Istat, censimento permanente delle imprese.

AREA	imprese attive con 10 e più addetti	imprese attive con 10 e più addetti che utilizzano software gestionale		imprese attive con 10 e più addetti che utilizzano servizi cloud	
		N.	%	N.	%
<b>Italia</b>	212.396	109.995	51,8%	46.977	22,1%
<b>Nord-ovest</b>	68.142	38.352	56,3%	16.664	24,5%
<b>Nord-est</b>	55.912	30.623	54,8%	13.423	24,0%
<b>Centro</b>	43.555	20.534	47,1%	9.089	20,9%
<b>Sud</b>	32.322	14.922	46,2%	5.456	16,9%
<b>Isole</b>	12.465	5.563	44,6%	2.346	18,8%

In questo contesto sono comprensibili gli sforzi della Commissione europea per ridurre le barriere all'adozione dei servizi cloud da parte delle imprese che sono legate principalmente ai temi della sicurezza e della protezione dei dati, ma anche all'incertezza circa il luogo in cui i dati risiederanno, e conseguentemente circa la giurisdizione applicabile in caso di contenzioso.

In aggiunta, la Commissione nel 2016 stimava che il valore totale dei servizi cloud nel 2020 in Europa sarebbe stato di 44,8 miliardi di euro, ma soprattutto che nel corso del periodo 2016 – 2020 tali servizi avrebbero accresciuto il prodotto interno lordo dei paesi EU28 di circa 449 miliardi di euro e avrebbero contribuito alla creazione di circa 300.000 nuove imprese (soprattutto piccole e medie)<sup>22</sup>.

Un'analisi dal punto di vista delle imprese, per comprendere le determinanti dell'adozione di servizi cloud da parte di queste ultime, consente di affermare che l'interesse delle imprese deriva dal fatto che i servizi cloud permettono il trasferimento delle principali funzioni IT in data center in cui ogni macchina fisica ospita un numero – spesso molto elevato – di server virtuali. Questo paradigma tecnologico, grazie al quale non si deve più allocare a ciascun server una macchina fisica, permette il conseguimento di significative:

- economie dal lato dell'offerta, dal momento che all'aumentare della dimensione del data center si riducono i costi per singolo server;
- economie dal lato della domanda, dal momento che i costi dipendono dall'utilizzazione delle risorse IT e che i carichi di lavoro si presentano in maniera

<sup>22</sup> Measuring the Economic Impact of Cloud Computing in Europe – A Study prepared for the European Commission, 2016.

molto variabile nel corso del tempo, richiedendo in certi particolari periodi ampie quantità di risorse e praticamente nessuna risorsa nel periodo successivo, l'aggregazione della domanda di servizi di computing e la diversificazione può incrementare il tasso di utilizzo dei server;

- economie da *multi-tenancy*, dal momento che i costi di gestione delle applicazioni e dei server si riducono all'aumentare del numero di *tenants* (utenti).

Le economie dal lato dell'offerta derivano da vari fattori, fra i quali uno dei più rilevanti è quello relativo al rapporto fra scala di produzione e costi dell'energia elettrica (i quali arrivano a costituire anche il 20% del Total Cost of Ownership dei sistemi IT). Difatti, i gestori di data center più grandi (i cosiddetti hyperscaler) nell'ambito delle proprie infrastrutture, che a volte hanno anche un'estensione mondiale, hanno maggiore facilità a localizzare i propri impianti nelle zone dove i costi dell'elettricità sono più bassi e, più in generale, dispongono di una maggiore capacità di negoziazione con i fornitori energia elettrica, il che si traduce in costi (e prezzi) più bassi. Lo stesso discorso vale anche per i costi del lavoro: benché i servizi cloud permettano una riduzione dei costi del lavoro ad ogni scala di produzione, grazie all'automazione di numerose attività di amministrazione di sistema, questa riduzione diviene ancor più marcata al crescere della scala di operazioni<sup>23</sup>.

Anche i costi relativi alla sicurezza ed all'affidabilità dei sistemi, richiedendo in larga parte investimenti fissi, mostrano rilevanti economie di scala. Infine, i gestori di data center di grandi dimensioni possono, grazie al proprio potere di acquisto, ottenere sconti sul software e sull'hardware che possono arrivare anche al 30%.

Le economie dal lato della domanda derivano fondamentalmente da efficienze nell'utilizzo delle risorse IT. Difatti, i costi dell'IT dipendono non solo dalla capacità di calcolo dei sistemi, ma anche dal grado di efficienza con cui tale capacità viene utilizzata. In un data center tradizionale, non virtualizzato, ogni carico di lavoro, ogni applicazione, "gira" sul proprio server fisico, il che significa che il numero dei server varia in proporzione al numero dei carichi di lavoro. Secondo questo modello, però, i server tipicamente operano ad un tasso di utilizzazione molto basso, anche inferiore al 10%.

Siccome in un sistema cloud più server sono virtualizzati su un numero inferiore di macchine, oltre a ridursi il numero di macchine fisiche necessarie, è possibile anche sfruttare la variabilità dei carichi di lavoro. Vi saranno infatti carichi di lavoro che in un certo momento richiedono molte risorse di sistema, ma che subito dopo non ne

---

<sup>23</sup> Microsoft (James Hamilton, Microsoft Research, 2006) stima che un amministratore di sistema in un'impresa tradizionale può gestire circa 140 server, lo stesso amministratore in un cloud data center ne può gestire migliaia.

richiedono alcuna; in questo contesto si possono conseguire economie significative attraverso l'aggregazione e la diversificazione della domanda.

Difatti, in un cloud virtualizzato in cui le risorse sono aggregate, in primo luogo si riduce – rispetto ad un sistema basato su server fisici – la necessità di prevedere su ciascun server una certa riserva di capacità per far fronte ad improvvisi picchi di domanda (più utenti che effettuano la stessa operazione nel medesimo momento).

Dal momento poi che i carichi di lavoro presentano un profilo orario (ad esempio, le attività business si concentrano durante il giorno, quelle consumer durante la sera), se si riserva per ciascuna categoria di applicazioni una macchina fisica, si rischia di tenerla inutilizzata per parte della giornata, ma se il medesimo server (o gruppo di server) viene utilizzato per entrambe le categorie, oppure si utilizzano i medesimi server per la medesima tipologia di carichi di lavoro, ma su differenti fusi orari, si può incrementare significativamente il tasso di utilizzo dei server.

Un'altra fonte di variabilità che può essere sfruttata per aumentare il tasso di utilizzo dei server è quella relativa alla stagionalità delle attività: vi sono industrie come quelle retail che presentano picchi nella stagione natalizia, altre, come la consulenza fiscale, si concentra in ben precisi periodi dell'anno. Utilizzando i medesimi server per entrambe le attività incrementerà il tasso di utilizzo delle infrastrutture.

Infine, dal momento che le risorse di calcolo (CPU), di storage e di Input/Output sono solitamente presenti sui server in bundle di proporzioni fisse, e che vi sono carichi di lavoro che utilizzano molte risorse di calcolo e poche di storage o di I/O e, viceversa, vi sono carichi che utilizzano molte risorse di storage e poche di calcolo, è possibile conseguire efficienze facendo girare in contemporanea carichi di lavoro con profili di utilizzo delle risorse complementari.

Alle economie di scala dal lato della domanda e dell'offerta, che sono conseguibili a prescindere dall'architettura delle applicazioni, si aggiungono le economie da *multi-tenancy*, le quali invece si conseguono solo se le applicazioni sono espressamente progettate per essere eseguite in un ambiente *multi-tenant*, ossia un ambiente in cui non è necessario avviare un'istanza di una determinata applicazione (si pensi ad un applicativo Office) per ciascun cliente, ma si può avviare un'unica istanza di un'applicazione che viene utilizzata da più utenti simultaneamente (come nel caso di Office 365 condiviso).

La *multi-tenancy* può generare risparmi nei costi del lavoro, dal momento che a differenza degli ambienti *single-tenant* in cui la gestione delle applicazioni (ossia le attività necessarie ad aggiornare le applicazioni, applicarvi patch e risolvere problemi) deve essere svolta per ogni singola istanza, negli ambienti *multi-tenant* i costi di gestione degli applicativi sono condivisi tra tutti gli utenti che utilizzano una singola

istanza, spingendo i costi verso il basso.

In aggiunta, la *multi-tenancy* permette anche di ridurre le risorse accessorie (*overhead*) che vengono solitamente riservate per far funzionare le applicazioni. Queste risorse, in un ambiente multi-tenant vengono ammortizzate fra tutti gli utenti dell'istanza.

Microsoft stima (Harms e Yamartino, Microsoft Research, 2010) che la combinazione delle economie dal lato dell'offerta, della domanda e di *multi-tenancy* può condurre a sensibilissimi risparmi nel TCO: le simulazioni di Microsoft mostrano come un cloud datacenter da 100.000 server, rispetto ad un datacenter da 1000 server può conseguire economie dell'ordine dell'80%, liberando risorse che possono essere utilizzate per l'innovazione o impiegate in altre attività.

Va comunque detto che la riduzione dei costi operativi non è l'unica ragione per la quale le imprese decidono di avvalersi di servizi cloud. Fra le ragioni si annoverano anche:

- la cosiddetta elasticità, ossia la capacità di scalare rapidamente – e senza variazione dei costi unitari – verso l'alto o verso il basso le risorse di calcolo (l'uso di 1000 server per un'ora costa più o meno quanto l'uso di 1 server per mille ore) che permette di dare avvio a progetti prima considerati troppo costosi o troppo lunghi da intraprendere;
- la riduzione dei costi capitali che riduce i costi di avvio o anche di abbandono dei progetti favorendo al contempo la sperimentazione;
- la *self provision*, ossia la capacità di mettere in piedi uno o più server tramite un portale anziché tramite complesse procedure di selezione dei fornitori e di approvazione delle spese accelera i tempi di fornitura (e di realizzazione dei progetti).

Quanto detto finora circa la scala di operazioni deve però essere temperato dal fatto che le imprese, come si è detto in precedenza, seguono spesso strategie multi-cloud e/o di cloud ibrido che prevedono, per almeno parte delle esigenze di queste ultime, il ricorso a servizi di cloud privato, anzi, come è possibile evincere dall'ultimo State of the Cloud report di Flexera<sup>24</sup>, relativo all'anno 2020, tali strategie rappresentano la norma più che l'eccezione<sup>25</sup>.

---

<sup>24</sup> Il rapporto è stato realizzato mediante interviste a 750 manager ed utenti di servizi cloud di tipo pubblico, privato ed ibridi. I risultati devono essere interpretati considerando che gli intervistati fanno capo ad aziende con un numero di addetti superiore a mille e che solo il 20% fa capo ad aziende europee (fronte di un 64% che fa capo ad aziende delle Americhe).

<sup>25</sup> Il 93% dei partecipanti alla survey su cui si basa il rapporto di Flexera ha dichiarato di adottare strategie multi-cloud, e quel 93% di partecipanti è costituito da un 87% che ha dichiarato di seguire strategie di cloud ibrido e da un 6% che ha dichiarato di seguire strategie di multi-cloud pubblico.

Se da una parte è vero che i servizi di cloud privato sono in grado di fornire risposta alle preoccupazioni delle imprese circa il trasferimento dei propri dati su cloud pubblici, dall'altra è anche vero che i servizi privati, pur continuando a beneficiare della virtualizzazione e della conseguente automazione della gestione di sistema, operano ad una scala inferiore e con meno possibilità di diversificazione dei carichi di lavoro. Ad esempio, la variabilità derivante dalla stagionalità delle attività all'interno di una singola industria non potrà essere diversificata e quindi le relative efficienze non potranno essere conseguite.

Da tutto ciò deriva che i costi del cloud privato possono essere anche sostanzialmente superiori a quelli del cloud pubblico per cui si viene a creare un trade-off tra esigenze di privacy, che spingono verso il cloud privato e costi, che spingono verso il cloud pubblico. In quest'ottica è possibile che l'iniziativa Gaia-X, creando un'infrastruttura federata basata su valori europei, volta a massimizzare la sovranità dei dati attraverso l'interoperabilità e la "security and privacy by design", possa ridurre, o comunque incidere, su questo trade-off e che possa anzi fornire nuove opportunità a quegli operatori di servizi cloud (a cominciare dalle Telco) localizzati all'interno dei confini europei le cui infrastrutture al momento risultano in buona parte inutilizzate perché gli utenti preferiscono i servizi cloud di operatori extra-UE. Ad ulteriore supporto di questa tesi vi è la già citata tendenza delle infrastrutture cloud a spostarsi verso l'edge della rete che potrebbe favorire accordi fra le Telco ed i grandi fornitori di servizi cloud.

Appare infine opportuno rilevare che affinché il mercato dei servizi cloud si sviluppi (e quindi anche iniziative quali Gaia-X possano aver successo) è però necessario che le imprese siano messe nelle condizioni di cambiare agilmente fornitore di servizi cloud trasferendo sui nuovi server non solo i propri dati, ma anche i propri ambienti informatici, applicativi, etc.

Per questo è necessario che si riesca a convergere in breve tempo su un insieme di standard ben definiti: difatti, benché grazie all'uso di tecniche basate su "container" (quali Docker o Kubernetes) sia possibile trasferire da un cloud provider ad un altro le proprie applicazioni ed i carichi di lavoro, nonché ad eseguire applicazioni su architetture altamente distribuite, nella pratica ciò non risulta sempre agile.<sup>26</sup> In questo un ruolo importante potrà essere giocato da Gaia-X, che oltre a favorire la convergenza verso un insieme di standard, si propone di creare un *framework* comune a tutti i domini verticali (industria, finanza, mobilità, green deal, energia, settore pubblico, telecomunicazioni) che dovrebbe facilitare la creazione di un ecosistema di servizi avanzati di intelligenza artificiale, big data analytics, etc. e contribuire all'innovazione.

---

<sup>26</sup> Il già citato rapporto "State of the Cloud 2020" di Flexera riporta che in media ciascuna imprese si avvale di 2,2 fornitori di servizi di cloud pubblico e 2,2 fornitori di servizi di cloud privato.

La creazione di questo ecosistema potrebbe facilitare il trasferimento dei dati delle imprese da un fornitore di servizi cloud ad un altro, eliminando fenomeni di lock-in.

### **3.3. Il cloud per la Pubblica Amministrazione: indicazioni per l'esperienza italiana**

#### **3.3.1. La storia dell'informatica nella PA: cenni**

Nel corso degli anni, le amministrazioni pubbliche del Paese hanno sviluppato una grande varietà di sistemi informatici a supporto dei propri processi istituzionali, sia a livello centrale che locale. In molti casi, ciò è avvenuto sviluppando applicativi *custom*, operanti su infrastrutture tecnologiche gestite direttamente dalla singola amministrazione. Ciò ha richiesto la creazione di propri centri di calcolo per ospitare le infrastrutture tecnologiche necessarie all'operatività di tali applicazioni. Con il tempo, alcuni servizi sono stati affidati in *outsourcing* a soggetti di mercato (*system integrators*), mentre altri sono stati affidati a società pubbliche create appositamente per la gestione di tali sistemi. Nella gran parte dei casi, tali sistemi hanno continuato (e continuano) ad operare in centri di calcolo e su macchine della singola amministrazione.

Per abilitare il reale cambiamento e l'innovazione del funzionamento delle nostre amministrazioni è necessario non solo ripensare la natura e le funzioni di questi sistemi informativi, ma anche far evolvere le infrastrutture tecnologiche e le relative strategie di gestione e *procurement*, al fine di cogliere le opportunità che sono oggi offerte dallo sviluppo del mercato ed eliminare una serie di problemi quali la scarsa sicurezza di molti impianti informatici in esercizio, i loro costi elevati e la difficoltà di evoluzione e crescita del parco applicativo.<sup>27</sup>

Da questo punto di vista, è vitale che le amministrazioni del Paese possano contare su una strategia organica di adozione dei moderni servizi e delle tecnologie del cloud computing, adozione che permetterebbe anche una riduzione e dismissione di Centri Elaborazione Dati (CED) e strutture civili, i quali in molti casi, risultano decisamente obsoleti.

Le opzioni a disposizione delle amministrazioni pubbliche si basano su due principali casistiche, prima richiamate:

---

<sup>27</sup> Su questi temi Astrid ha avviato una riflessione già nel 2011 con la pubblicazione del libro su "[\*Pubblica Amministrazione che si trasforma: Cloud Computing, federalismo interoperabilità\*](#)", a cura di Enrico Acquati, Simona Macellari e Alessandro Osnaghi, prefazione di Franco Bassanini e Roberto Masiero, Passigli Editori, 2011.

1. Cloud privato: utilizzo di infrastrutture detenute e gestite direttamente da amministrazioni pubbliche o loro enti e società delegate.
2. Cloud pubblico: utilizzo dei servizi offerti da operatori di mercato.

Il cloud privato garantisce che le informazioni e i servizi informativi operino e siano gestiti sotto il pieno controllo della singola amministrazione. Il cloud pubblico permette di ottimizzare costi, incrementare la flessibilità nell'utilizzo dei servizi infrastrutturali, sfruttare le esperienze e le tecnologie dei leader a livello mondiale nel settore.

Dal punto di vista delle amministrazioni pubbliche, vi sono casi dove è opportuno o necessario mantenere i sistemi su un cloud privato. In altri casi, l'utilizzo del cloud pubblico può portare una serie di benefici significativi e deve quindi essere certamente considerato. In realtà, i casi nei quali è realmente necessario utilizzare un cloud privato sono limitati e quindi ha senso ipotizzare un crescente ed ampio utilizzo del cloud pubblico.

In generale, è opportuno che le amministrazioni pubbliche possano usufruire di entrambe le opzioni. In ogni caso, è vitale che tutte le amministrazioni che oggi hanno sistemi e impianti in situazioni critiche debbano e possano migrare verso soluzioni che garantiscano sicurezza, privatezza, continuità e gestione organica del servizio.

Per quanto riguarda il cloud privato, oggi alcuni attori pubblici detengono già infrastrutture in grado di offrire questo servizio (per esempio, SOGEI a livello centrale e diverse *in-house* regionali o locali). Alcune di queste infrastrutture sono di qualità e possono certamente costituire una risorsa utile; altre sono obsolete e andrebbero dismesse. In generale, ha senso pensare ad una razionalizzazione che qualifichi una serie di attori pubblici in grado di offrire servizi di cloud privato di qualità.

Dal punto di vista del cloud pubblico, ha senso prevedere un supporto alle amministrazioni che vogliano poter usufruire dei servizi offerti dagli operatori di mercato.

Nei mesi scorsi, è emersa l'intenzione del Governo di creare uno Polo Strategico Nazionale (PSN) che si occupi di offrire servizi di *cloud computing*. Dai documenti finora disponibili, emerge una serie di punti che necessitano di ulteriori approfondimenti per poter esprimere un giudizio su questa proposta. Se ne evidenziano alcuni, per i quali è utile un confronto con i partner di questa ricerca.

- i. Il PSN è una struttura che dispone di proprie infrastrutture oppure agisce da broker di servizi esistenti?
- ii. Nel secondo caso, si tratta solo di servizi cloud privati o anche di servizi di cloud pubblici?
- iii. Chi deve utilizzare necessariamente i servizi del PSN e perché?

iv. Il PSN offre i propri servizi anche a privati?

In generale, al momento, non è chiaro quali siano natura, criteri di funzionamento e obiettivi del PSN e, soprattutto, il rapporto che esso stabilirebbe con gli attori esistenti.

### ***3.3.2. La razionalizzazione dei servizi informativi delle Amministrazioni Pubbliche***

L'utilizzo del cloud, pubblico o privato che sia, non è semplicemente una operazione che coinvolge le infrastrutture tecnologiche e la gestione degli impianti (CED). Per utilizzare i servizi cloud, sono innanzi tutto necessari un ripensamento, una ristrutturazione ed un consolidamento del parco applicativo, così da renderlo adatto ad una migrazione verso le piattaforme e i servizi cloud.

Purtroppo, in questi anni il dibattito e le proposte si sono concentrate sul tema della "riduzione e consolidamento dei CED", senza considerare che - in assenza di un consolidamento del parco applicativi - l'operazione sui CED si riduce ad essere poco più di un trasloco di macchine, mentre la vera migrazione non può nei fatti avvenire.

Per questi motivi è vitale che si definisca quanto prima un piano di consolidamento e razionalizzazione del parco applicativo delle amministrazioni pubbliche e si definisca una strategia di reingegnerizzazione dei sistemi da migrare al fine di renderli effettivamente compatibili con le piattaforme cloud, private o pubbliche che siano.

Alla luce di quanto precede, sembra opportuno, se non inevitabile, che sia riesaminato l'approccio seguito per il progetto di cloud nazionale per la Pubblica Amministrazione, previsto dal Decreto Semplificazioni ed ora, come detto, divenuto uno dei progetti del PNRR.

## **Capitolo 4. Prime considerazioni conclusive**

### **4.1. Quale strategia industriale per il cloud europeo: oltre il "campione europeo del cloud"**

Era previsto che entro questo mese, aprile 2021, la *European Alliance on Industrial Data and Cloud* presentasse le proposte di linee guida sulle key priorities prima richiamate. In questa sede, in questo momento, il gruppo di lavoro non ha preso in considerazione questi sviluppi, peraltro non noti. Invece, il gruppo di lavoro si esercita – in via del tutto teorica – sui possibili percorsi di una politica industriale europea per il cloud, con specifico riferimento alla prospettiva di promuovere un operatore in concorrenza con le grandi imprese di USA e Cina.

In linea di principio, appare condivisibile un rafforzamento dell'industria europea del

cloud e dei dati che passi anche attraverso la sinergia di investimenti pubblici e privati. Tuttavia, l'ipotesi di costituire un "campione europeo del cloud", capace di competere con le grandi aziende americane e cinesi, appare velleitaria. Ciò per diverse ragioni.

In primo luogo, l'industria europea sconta un ritardo nel mercato del cloud quantificabile in 10-15 anni rispetto ai grandi operatori internazionali. Questo ritardo appare oggettivamente incolmabile, soprattutto considerato che questo settore è investito da continui progressi tecnologici, ma anche da evoluzioni negli stessi modelli d'offerta, come rappresentato in precedenza. In altri termini, in questo caso, non sembra possibile il modello di innovazione *leapfrogging* che può consentire ai *newcomers* di sfidare le imprese consolidate sul mercato, grazie alla promozione di innovazioni di tipo radicale (*breakthrough*). Non si vede quali imprese possano farsi promotrici di innovazioni radicali che sfidino il potere di mercato delle grandi piattaforme digitali americane e cinesi, le quali, anzi, continuano ad essere il luogo privilegiato per nuovi sviluppi tecnologici.

In secondo luogo, una iniziativa volta alla costruzione di un "campione europeo" potrebbe incontrare – molto probabilmente - le perplessità della stessa Commissione europea, se questo progetto portasse ad una riduzione del grado di concorrenza nei singoli mercati nazionali.

In altri termini, andrebbero bilanciate due distinte esigenze, comunque riconducibili agli assetti di mercato. Per un verso, procedere alla costituzione di un nuovo protagonista nel mercato del cloud, attraverso una serie di *mergers & acquisitions*, accordi di collaborazione o la costituzione di *joint ventures* darebbe un impulso alla concorrenzialità del mercato, almeno a livello continentale. Per altro verso, questo processo potrebbe tuttavia ridurre il numero di alternative presenti nei diversi mercati, riducendo il potere contrattuale dei clienti e, anche, disincentivando la nascita di nuove imprese.

Inoltre, esiste un problema di equilibrio "politico", nel senso che – assai probabilmente – il "campione europeo" sarebbe un "campione francese" o tutt'al più "franco-tedesco". Le ultime iniziative di mercato dell'operatore Atos potrebbero essere lette nella direzione di rafforzare questo particolare soggetto, candidandolo a volgere il ruolo di "*European champion*" del cloud. Se questa fosse la dinamica, il nostro paese, ma anche gli altri, dovrebbero chiedersi se l'indipendenza digitale dell'Europa dalle grandi imprese americane e cinesi sarebbe in tal modo effettivamente risolta.

Da ultimo, può essere utile richiamare l'esperienza francese in materia di cloud nazionale, come precedente non certo *successful*.

L'idea di creare e gestire dei datacenter sul suolo francese, per ospitare i dati della

pubblica amministrazione, è del 2009, ed il progetto – denominato Andromède – viene avviato due anni dopo. L'obiettivo dichiarato era di riservare a società francesi le responsabilità in materia di sicurezza, affidabilità e gestione dei sistemi, eliminando così il rischio di un accesso a dati strategici della PA francese (ma anche di imprese francesi ed europee) da parte di soggetti esterni.

Lo strumento di realizzazione del progetto era immaginato come una partnership pubblico privato, con la partecipazione dei maggiori operatori dei mercati ICT, ma con lo Stato in qualità di primo azionista.

Controversie tra i diversi soggetti privati hanno impedito al progetto Andromède di trasformarsi in realtà, mentre l'idea di un cloud "sovrano" ha poi trovato forma in due distinte società, Cloudwatt e Numergy.

La prima (Cloudwatt) si è realizzata con la partecipazione di Orange e Thales, la seconda (Numergy) di SFR e Bull. In entrambi i casi, lo Stato è intervenuto, acquisendo il 33% del capitale, tramite la Caisse des Dépôts et Consignations.

La presenza dello Stato è tuttavia durato poco: già nel 2015, Cloudwatt è diventata un'impresa di Orange e Numergy è stata acquisita da SFR.

Dal punto di vista del modello di business, entrambe le società, Cloudwatt e Numergy, adottano una soluzione ibrida, con un'offerta rivolta sia alla PA, sia alle imprese private. In tal modo, di fatto è stata superata l'idea iniziale del progetto Andromède di prevedere un'offerta mirata alla sola PA.

In conclusione, l'intervento pubblico è servito – alla fine – a sostenere il rafforzamento di due importanti operatori di TLC nel mercato del cloud. Un esito che va considerato con riguardo agli impatti di mercato e concorrenziali, non solo con riferimento alla sfida agli *hyperscaler*, ma anche alle società di minori dimensioni che pure operano nei mercati cloud.

Un diverso discorso, che per ora si accenna soltanto, può invece coinvolgere la domanda, piuttosto che l'offerta di servizi cloud.

In tal senso, si potrebbe pensare ad una federazione dei principali utilizzatori di servizi cloud, sia che abbiano sviluppato cloud privati, sia che ricorrano a cloud pubblici. In estrema sintesi, questa federazione si presenterebbe davanti ai grandi fornitori con un potere contrattuale rafforzato, e sostenuto da una disciplina, necessariamente europea, che definisca le regole per la fornitura di servizi cloud, nel rispetto dei valori europei in materia di sicurezza, privacy, proprietà dei dati, tutela dell'ambiente.

A tale proposito, è di fondamentale importanza seguire e, per quanto possibile, indirizzare l'evoluzione del progetto Gaia-X.

## 4.2. La natura e il ruolo di Gaia-X

Dal sito dell'Associazione, si apprende che Gaia-X è un progetto “promosso dall'Europa per l'Europa ed oltre. Il suo obiettivo è sviluppare requisiti comuni per una infrastruttura europea dei dati. Perciò, apertura, trasparenza, e la possibilità di collegarsi ad altri paesi europei sono centrali per Gaia-X”.

La natura di Gaia-X va definendosi meglio a mano a mano che l'Associazione procede nella sua operatività: intanto, con la nomina del gruppo dirigente. Ad oggi, tuttavia, sembrano esservi ancora aspetti non del tutto definiti che, quindi, rendono ancora plausibili i diversi possibili paradigmi e scenari da cui è partito il gruppo di lavoro:

1. Opzione “GSM-like”: in questo scenario, Gaia-X è un insieme di standard di qualità, sicurezza e interoperabilità che qualifica le offerte esistenti, rendendole allo stesso tempo sostituibili e intercambiabili.
2. Opzione “Airbus-like”: in questo scenario, Gaia-X è un attore di mercato che offre con proprie strutture servizi cloud in competizione con gli attuali attori del mercato.
3. Opzione “ibrida”: in questo scenario Gaia-X definisce un ruolo di standardizzazione e di brokeraggio verso i servizi di mercato.

Nell'opzione 1, Gaia-X non svolge un ruolo attivo durante il processo di fruizione del servizio, lasciando la gestione complessiva al fornitore che aderisse ai suoi standard. Nell'opzione 2, Gaia-X è un attore di mercato che con le proprie infrastrutture e capabilities offre servizi a clienti pubblici e privati.

L'opzione 3 potrebbe essere attivata in forma selettiva per alcuni segmenti di mercato. Per esempio, nel caso delle amministrazioni pubbliche, si potrebbe costituire un veicolo ad-hoc che (con un orizzonte temporale non superiore ai 5-10 dieci anni) acquisisse tramite procedura pubblica servizi dal mercato e li erogasse con una governance e gestione mista pubblico-privata, al fine di tutelare in modo rafforzato il cliente pubblico per applicazioni critiche per le quali non risultassero sufficienti le clausole contrattuali e i modelli di gestione tradizionali offerti dai provider di servizi di cloud pubblico.

Peraltro, questa opzione potrebbe essere a sua volta esplicitata (almeno) in due modi diversi: nel primo caso la procedura pubblica seleziona “una tantum” ed a monte uno o più fornitori che costituiscono il nucleo privato della partnership pubblico-privata; nel secondo caso, la procedura definisce una serie di vincoli, processi e requisiti e tutti i fornitori che in qualunque momento risultassero conformi con tali requisiti potrebbero rientrare come partner e fornitori dei servizi. Nel secondo caso, ci troveremmo di fronte ad una opzione che di fatto costituisce un rafforzamento ed istituzionalizzazione dell'opzione 1 (esiste un soggetto gestore), con requisiti e vincoli particolarmente

stringenti per uno specifico settore di mercato.

Ad avviso del gruppo di lavoro, appare impraticabile perseguire l'opzione 2, ossia il modello Airbus, mentre le opzioni 1 e 3 potrebbero da un lato garantire maggiore tutela per gli utenti europei e, dall'altro, aprire la strada a possibili attori europei che, partendo magari da settori di nicchia, siano in grado di divenire nel tempo una alternativa credibile agli incumbent statunitensi.

Si è – tuttavia – accennato che, seguendo i lavori di Gaia-X, va delineandosi come, oltre il profilo regolamentare, in ogni caso diverso da quello tipico degli enti di standardizzazione (ad esempio, ETSI, per le telecomunicazioni), l'Associazione si è data l'obiettivo di realizzare una infrastruttura *software* posta logicamente al di sopra delle infrastrutture fisiche di cloud. In questo modo, si entra nel campo dell'intervento industriale, attraverso la promozione di un nuovo protagonista europeo del cloud. Questo soggetto si configurerebbe come un abilitatore di una federazione di più “nodi” (evitando comunque la iper-concentrazione), rispettoso dei criteri di affidabilità e sovranità, grazie all'uso di meccanismi software, definiti dal progetto Gaia-X, che garantirebbero visibilità e controllo sull'utilizzo dei dati ed una regolamentazione il più possibile automatica e basata sul consenso distribuito.

In questo contesto, si sta sviluppando un progetto, questa volta per la realizzazione di una nuova infrastruttura fisica, nell'ambito dell'Alleanza su Cloud e Industria dei dati, finanziata tramite un progetto IPCEI sul cloud<sup>28</sup>.

Questo tema, assieme a quello della piattaforma software di Gaia-X, merita specifici approfondimenti, che saranno svolti nella prosecuzione delle attività del gruppo di lavoro.

Dal punto di vista delle strategie delle amministrazioni pubbliche italiane, sarebbe poi utile che i chiarimenti relativi al PSN venissero sviluppati tenendo conto dell'evoluzione dell'iniziativa Gaia-X.

Come dimostrano le prime otto aree di business individuate da Gaia-X per garantire sicurezza e privacy dei dati,<sup>29</sup> l'esposizione non riguarda solo una categoria: tutti i settori chiave dalle corporate alla sanità, con tutti i dati sensibili e privati di cui dispongono, sono esposti e necessitano protezione.

I dati sono la risorsa strategica per la digitalizzazione dell'economia e lo diventeranno ancor di più, man mano che le Industrie 4.0 e IoT cresceranno di importanza, portando in primo piano il ruolo delle piattaforme e dello scambio dei dati, come vettori di innovazione in ambiti strategici, dalla ricerca, all'intelligenza artificiale. Sfruttare al

---

<sup>28</sup> <https://www.europeancloudalliance.com/>

<sup>29</sup> Energia, finanza, salute, Industria 4.0/PMI, agricoltura, mobilità, settore pubblico, domotica.

meglio questa preziosa risorsa diventa l'obiettivo primario degli ecosistemi aziendali, di qualsiasi natura.

Ed è a tal proposito, in difesa della sicurezza di aziende e Stati, che si richiama il concetto di "sovranità dei dati europea" che Gaia-X dovrebbe valorizzare, insieme ad autonomia strategica e difesa degli interessi europei: quel ruolo competitivo nel Cloud che l'Europa ancora non è riuscita a giocare.

Negli ultimi anni, l'Unione Europea è intervenuta attivamente per introdurre aspetti normativi rilevanti, innalzare gli standard di privacy e di regolamentazione ma non nello sviluppo di credenziali tecnologiche (in termini di investimento e di ricerca e sviluppo) per competere con le altre superpotenze, come la Cina e Stati Uniti: un gap infrastrutturale che Gaia-X cerca di compensare.

L'opportunità generata da un'infrastruttura UE efficace e sovrana in cui i dati possano essere condivisi e archiviati secondo gli standard di protezione europei, apre diversi scenari; può infondere a industria e cittadini maggior fiducia nel modo in cui i dati vengono elaborati. Nel lungo periodo, il Cloud condiviso potrebbe favorire lo sviluppo anche delle imprese più piccole, in settori che vanno dalla finanza all'energia, concedendo loro l'opportunità di presentarsi sulla scena globale e di sfruttare le potenzialità innovative dei dati, oltre che da parte delle PA.

Rispetto alle prospettive di sviluppo dell'industria del Cloud, l'accento è, da più parti, posto sull'importanza della valorizzazione (e successiva monetizzazione) dei dati che vengono conservati nel Cloud. Più che la questione di residenza dei dati sul territorio nazionale, la vera sfida appare – appunto – quella di garantire la proprietà e la valorizzazione dei dati prodotti da imprese e pubbliche amministrazioni, definendo una disciplina che affianchi ed integri le previsioni del Regolamento Generale sulla Protezione Dati (GDPR) che sono limitate ai dati personali.

A questo proposito, è di fondamentale importanza affrontare il tema della classificazione dei dati, come accaduto ad esempio nell'esperienza di alcuni paesi europei (Regno Unito) e degli Stati Uniti. La classificazione dei dati è infatti un punto di partenza importante per determinare quale livello di controllo appropriato applicare alla tipologia di dato in termini di riservatezza, integrità e disponibilità in base ai rischi dell'organizzazione proprietaria del dato.

Sempre sotto il profilo del ruolo della Pubblica amministrazione italiana in particolare, nell'ambito della strategia cloud che il nuovo Ministro per l'Innovazione e la Transizione Digitale dovrà definire, diventa fondamentale tenere conto anche della sinergia tra la struttura abilitante ed il ruolo della Pubblica amministrazione nei processi di digitalizzazione, come verranno indicati nel PNRR (Piano Nazionale di Ripresa e Resilienza).

A questo riguardo, si deve ricordare come l'azione di governo, sia a livello centrale che locale, è stata spesso centrata, anche recentemente, sulle nuove tecnologie da adottare e sullo sviluppo e sulla fornitura di servizi di front-end (portali, app, sistemi di pagamento, identità digitale) e non anche sul tema della reingegnerizzazione e della revisione dei processi e dei prodotti della PA<sup>30</sup>.

Un cambio di prospettiva di questo tipo creerebbe le condizioni per rendere finalmente possibile una comunicazione diretta tra amministrazioni e, dal punto di vista informatico, la piena interoperabilità dei back-end, il consolidamento delle basi di dati del Paese, la razionalizzazione del parco applicativi, premessa quest'ultima indispensabile anche per il passaggio al cloud e l'ottimizzazione dei centri di calcolo e dei sistemi di elaborazione delle amministrazioni.

In questa ottica, come già richiamato in precedenza, il pubblico dovrebbe sempre più concentrarsi sulla gestione degli asset strategici del Paese (base di dati e sistemi di back-end), lasciando spazio ai privati per quanto riguarda l'erogazione dei servizi di front-end. Nelle circostanze – assai particolari - in cui, invece, lo Stato decida di operare sul mercato con una propria offerta, si dovrà necessariamente confrontare con le condizioni del mercato, nel rispetto della regolazione vigente e delle norme antitrust.

---

<sup>30</sup> Si tratta di temi (in particolare la distinzione tra front-end e back-end e il bisogno di far interoperare i back-end delle PA per sviluppare front-end veramente utili) già presenti nel Piano d'azione per *l'e-gouvernement* elaborato nel 1999 dal prof. Alessandro Osnaghi su mandato del Ministro per la Funzione Pubblica Franco Bassanini e presentato nel 2000.