



UNIVERSITÀ
DI PAVIA

Dipartimento di Scienze Economiche e Aziendali

**Corso di Laurea Magistrale in
Economia e Gestione delle Imprese**

**Analisi Critica dei Contratti
nel contesto del Cloud Computing:
un Approccio Normativo ed Economico**

Relatore:

Chiar.mo Prof. Gabriele Faggioli

**Tesi di Laurea
di Sara Abdullah
Matr. n. 513975**

Anno Accademico 2023-2024

Indice

Introduzione.....	6
Contesto cloud computing	6
Perché è importante analizzare i contratti di cloud computing?.....	7
Capitolo 1 - Caratteristiche del cloud computing	9
1.1 Definizione cloud computing e le sue caratteristiche	9
1.2 Principali modelli.....	14
1.2.1 Software as a service – SaaS (Cloud applications).....	16
1.2.2 Platform as a service – PaaS (Cloud platforms)	17
1.2.3 Infrastructure as a service – IaaS (Cloud infrastructure).....	17
1.2.4 Hybrid (Multi-cloud)	18
1.3 Principali modalità di distribuzione	18
1.3.1 Public Cloud	19
1.3.2 Private Cloud	20
1.3.3 Community Cloud.....	21
1.3.4 Hybrid Cloud	22
1.4 Problematiche del cloud computing	24
1.4.1 Residenza dei dati e compliance.....	25
1.4.2 Lock in	27
1.4.3 Servizi standard.....	28
Capitolo 2 - Confronto contrattuale tra Modello Classico e Cloud Computing	29
2.1 Modello classico per realizzare sistema informativo.....	29
2.1.1 Molteplici contratti	29
2.1.2 Alta contrapposizione di obiettivi fra cliente e fornitore.....	33
2.1.3 Asimmetria informativa.....	34
2.1.4 Rischio del non accordo.....	35
2.1.5 Fattore tempo	38
2.1.6 Implementazione di un nuovo sistema informativo con Business Analyst.....	39
2.2 Prassi contrattuale per cloud computing.....	40
2.2.1 Asimmetria negoziale	40
2.2.2 Struttura contrattuale.....	42
2.2.3 Trasparenza	44
Capitolo 3 – Contratti cloud: aspetti giuridici ed economici nella scelta di fornitura	46
3.1 Il contratto cloud: specificità ed aspetti normativi	46
3.1.1 La responsabilità del cloud provider.....	51

3.1.2	Limitazioni ed esclusioni della Responsabilità del Cloud provider	54
3.2	Patologie nella gestione dei contratti cloud: ripercussioni legali ed economiche	56
3.3	Strategie di way out: diritto di risoluzione e recesso del contratto	60
3.4	L'azienda cliente: valutazione e scelta del cloud provider	62
Capitolo 4 –	British Airways & CBRE: analisi del caso	70
4.1	Contesto del caso: British Airways vs CBRE.....	70
4.2	Il ruolo del cloud computing nell'industria dell'aviazione.....	71
4.3	Il cloud computing in British Airways	73
4.4	CBRE: il servizio di cloud computing	75
4.5	La Controversia British Airways vs CBRE	79
Conclusione	82
Bibliografia.....		85
Articoli & Documenti.....		87
Sitografia		89

Introduzione

Contesto cloud computing

Le tecnologie di cloud computing sono diventate molto popolari tra le imprese e le pubbliche amministrazioni. Il motivo di tale successo è dovuto alla presenza di un'ampia gamma di servizi sul mercato che incentivano l'utilizzo di servizi esternalizzati consentendo a chi ne usufruisce di ottenere notevoli vantaggi derivanti dalla sostituzione o dall'integrazione degli asset aziendali tradizionali utilizzati per la gestione delle informazioni con soluzioni esterne, che possono essere acquistate su base di consumo da terze parti ¹.

Questa tendenza significativa è stata influenzata da una serie di fattori, tra cui quelli elencati di seguito:

- **Aumento dell'incertezza legata agli investimenti in IT dopo la crisi del 2008**

Tra gli effetti causati dalla crisi economica mondiale che ha avuto inizio nel 2008 vi è l'aumento dell'incertezza legata agli investimenti in IT. La maggior parte delle aziende ha cambiato strategia, sostituendo le complesse iniziative di trasformazione con servizi più veloci e di immediato recupero dell'investimento iniziale, come il “cloud computing” ².

- **Passaggio al lavoro da remoto accelerato dalla pandemia**

L'avvento della pandemia ha accelerato la trasformazione nei modelli di lavoro ed ha portato un rapido passaggio al lavoro da remoto per garantire la continuità operativa ³
⁴.

- **Aumento dell'e-commerce**

L'aumento dell'e-commerce ha reso indispensabile l'utilizzo di infrastrutture tecnologiche e non che presentino un elevato grado di flessibilità ed in grado di

¹ Faggioli, G., & Italiano, A. (2017). *I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider*. Franco Angeli.

² <https://bsolutionsgroup.it/2019/08/29/da-capex-a-opex-il-cloud-e-la-sua-evoluzione-al-servizio-del-business/#:~:text=Quando%20la%20crisi%20economica%20del,quindi%20le%20risorse%20a%20budget>.

³ <https://www.mdmtecnodocs.com/2021/11/il-cloud-al-tempo-del-covid-19/>

⁴ <https://www.smcconsulting.it/la-trasformazione-digitale-al-tempo-della-pandemia/>

garantire la gestione di picchi di traffico durante determinati periodi ^{5 6}.

Il continuo ricorrere a questa tipologia di servizi, può essere inquadrato anche dall'analisi di alcune determinate statistiche, quali ad esempio:

- Dal punto di vista prospettico, il cloud computing in termini di dimensioni passerà da 371,4 miliardi di dollari nel 2020 a 832,1 miliardi di dollari nel 2025, con un tasso di crescita annuale composto (CAGR) del 17,5% (*Fonte: Mercati e mercati*) ⁷.
- Entro il 2023, il 94% delle imprese aveva in cantiere il progetto di adozione di almeno un servizio cloud, con una media di 2,2 servizi cloud utilizzati nelle medie imprese e 4,8 nelle grandi aziende. (*Fonte: Flexera*) ⁸.
- La diffusione della COVID-19 ha aumentato l'uso della tecnologia cloud, poiché le organizzazioni hanno dovuto adattarsi rapidamente al lavoro a distanza. In un sondaggio condotto tra i responsabili delle decisioni in materia di IT, il 40% ha dichiarato di aver aumentato la spesa per il cloud a causa della pandemia (*Fonte: Flexera*) ⁹.

Perché è importante analizzare i contratti di cloud computing?

In questo contesto dinamico e in rapida evoluzione dove le imprese vogliono sempre più affidarsi al cloud computing è cruciale prestare attenzione ai dettagli dei contratti perché spesso caratterizzati da termini tecnici e clausole intricate. Comprendere appieno queste clausole contrattuali e i relativi termini tecnici è essenziale per mitigare rischi potenziali, garantire la protezione dei dati sensibili e stabilire relazioni durature con i fornitori di servizi cloud.

In questa tesi verranno esaminate le caratteristiche, le criticità e i confronti tra contratti di cloud computing al fine di comprendere il processo decisionale relativo all'ICT che gli attori

⁵ <https://www.semplesio.it/e-commerce-in-cloud-a-cosa-serve-e-quali-sono-i-vantaggi/>

⁶ [Nel terzo trimestre 2021 il commercio digitale in Italia è cresciuto del 15% e si prevede ancora un Natale da record per l'e-commerce, ma attenzione all'aumento dei prezzi - Salesforce](#)

⁷ [Lambert Consulting - Statistiche e tendenze in Cloud Computing 2023 - 2024](#)

⁸ [Lambert Consulting - Statistiche e tendenze in Cloud Computing 2023 - 2024](#)

⁹ [Lambert Consulting - Statistiche e tendenze in Cloud Computing 2023 - 2024](#)

aziendali compiono.

- Nel primo capitolo si parlerà del cloud computing, partendo dalla sua definizione e dalle sue caratteristiche fondamentali. Saranno poi analizzati i principali modelli di servizio del cloud (come SaaS, PaaS, IaaS e Hybrid) e quelli di distribuzione (come Public, Private, Community e Hybrid). Il capitolo si concluderà con l'illustrazione delle problematiche del cloud computing.
- Il secondo capitolo si occuperà di confrontare il modello classico di realizzazione di sistemi informativi con l'approccio contrattuale nel cloud computing. Lo studio prevede una vera e propria analisi comparativa che consente di evidenziare come l'approccio al cloud sia più agile rispetto a quello tradizionale ma, allo stesso tempo, possa essere anche più rischioso se la regolamentazione dello stesso rapporto cliente fornitore non avviene in maniera critica.
- Il terzo capitolo analizzerà dettagliatamente le considerazioni contrattuali nei servizi cloud. Quello che si vuole analizzare è come l'eventuale assenza di elementi critici da inserire in un contratto cloud possa avere delle ripercussioni di natura legale ed economica significative per l'azienda che usufruisce dei servizi cloud. Ad esempio, la mancata gestione degli SLA può portare a danni economici se un fornitore non rispetta le tempistiche critiche. Infatti, ciò che si analizzerà è come in tali contratti venga delineato il criterio di responsabilità, in modo da valutare, in sede di contenzioso, la responsabilità e i relativi impatti.
- Infine, nell'ultimo capitolo, si analizza il caso CBRE, società di servizi cloud, e British Airways, che ha subito delle ripercussioni negative a causa di un mancato servizio da parte di CBRE. Questo evento ha danneggiato l'intero sistema operativo di British Airways, causando all'impresa danni significativi. Verrà esposto come British Airways abbia gestito la necessità di dotarsi di un servizio cloud e come questo sia stato oggetto di negoziazione e gestione con CBRE.

Capitolo 1 - Caratteristiche del cloud computing

1.1 Definizione cloud computing e le sue caratteristiche

L'istituto nazionale degli standard americana (The National Institute of Standards and Technology – NIST – of the US Government), definisce il cloud computing come un modello per abilitare accessi senza barriere in termini di distanza che, allo stesso tempo, si mostrano essere vantaggiosi in quanto poggiati su richiesta ad un pool condiviso di specifiche risorse di calcolo configurabili (ad esempio, reti, server, storage, applicazioni e servizi), il tutto con un effort sostenuto per la loro implementazione e fruizione ¹⁰.

Invece, rispetto a quanto definito da Amazon Web Services, il cloud computing rappresenta la fornitura di risorse informatiche su richiesta mediante l'utilizzo di internet, con una modalità di pagamento basata su quello che è l'utilizzo effettivo delle risorse (anche se questo è un modello comune, non è l'unico possibile). Invece di investire nell'acquisto, nella proprietà e nella gestione di data center e server fisici, è possibile accedere a servizi tecnologici come capacità di calcolo, archiviazione e database secondo necessità, affidandosi a un fornitore di servizi cloud, quale ad esempio lo stesso Amazon Web Services (AWS) ¹¹.

Anche Google fornisce una definizione di cloud computing, descrivendolo come la disponibilità on demand di risorse di calcolo attraverso servizi su Internet. In questo modo, le aziende non hanno la necessità di procurarsi, configurare o gestire l'infrastruttura autonomamente e pagano solo per quello che utilizzano ¹².

L'opposto concettuale del cloud computing è l'approccio "on-premise" o "on-prem (in italiano si traduce con "in loco" o "in sede") e si riferisce alla gestione delle risorse informatiche direttamente all'interno della sede, anziché essere collocate in data center o

¹⁰ <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>

¹¹ <https://aws.amazon.com/it/what-is-cloud-computing/>

¹² <https://cloud.google.com/learn/what-is-cloud-computing?hl=it#:~:text=Cloud%20Computing%20Foundations-Definizione%20di%20cloud%20computing,come%20i%20servizi%20su%20Internet>

infrastrutture remote come avviene con il cloud computing ¹³. In un ambiente on-premise, l'azienda è responsabile dell'acquisto, della configurazione, della manutenzione e della sicurezza dell'intera infrastruttura hardware e software necessaria per supportare le proprie operazioni informatiche. Questo implica che sono necessari grossi investimenti e la scalabilità può essere limitata dalla capacità fisica dei server e delle risorse locali.

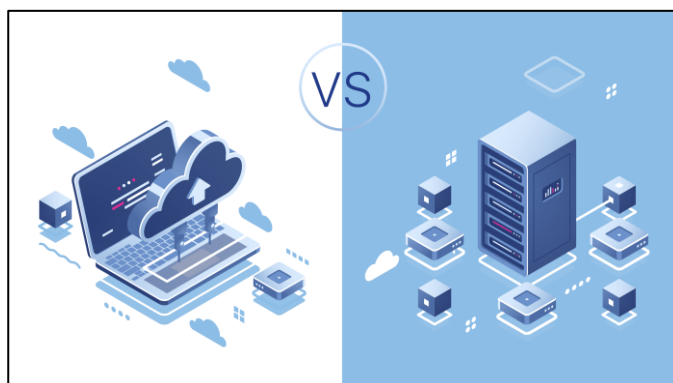


Figura 1 - "Differenza tra Cloud Computing e On-Premise: un confronto visivo"

Cloud Computing (a sinistra): è rappresentato da una nuvola, simbolo del cloud, questo modello mostra come le risorse hardware e software siano erogate attraverso una rete globale. L'accesso è flessibile, il pagamento è basato sull'effettivo utilizzo e la scalabilità è rapida ed efficiente.

On-Premise (a destra): è rappresentato da una struttura fisica, questo modello evidenzia come le risorse siano gestite all'interno delle strutture aziendali. Gli investimenti iniziali sono significativi, si è responsabili della manutenzione e si hanno limitazioni in termini di scalabilità (legate alla capacità fisica dei server locali).

Grazie all'avvento delle piattaforme cloud, coloro che utilizzano i loro servizi possono utilizzare risorse hardware e software messe a disposizione da terze parti in modo semplice e con un notevole risparmio in termini economici. Questi fattori sono alla base della diffusione del "cloud computing" a livello globale, sia per le piccole imprese che per le medie e grandi imprese.

¹³ Lezioni di organizzazione dei sistemi informativi dell'azienda del Professore Francesconi e di metodologie e tecniche dell'impresa digitale del Professore Del Vecchio

Il processo di conversione e migrazione dei dati, delle applicazioni e dei servizi IT da ambienti on-premise a soluzioni basate su cloud computing si chiama "cloudification" ed è uno dei tanti processi che rientrano nella trasformazione digitale.

Il cloud computing è un modello di servizio che offre una serie di caratteristiche chiave che lo rendono una scelta affidabile e conveniente per molte organizzazioni ¹⁴. Le caratteristiche sono:

- Elasticità e scalabilità rapide,
- Automatizzazione,
- Multi-tenancy e resource pooling,
- Ampio accesso alla rete,
- Servizio misurato e segnalato,
- Struttura di pagamento basato sull'uso,
- Facile manutenzione,
- Resilienza,
- e infine, Sicurezza per la protezione dei dati.

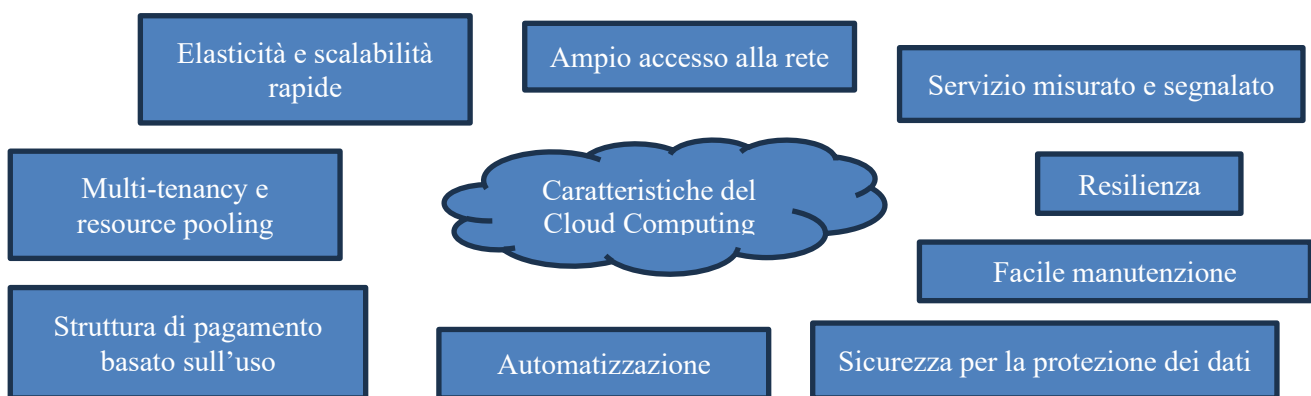


Figura 2 - Caratteristiche del cloud computing ^{15 16 17 18 19}

¹⁴ <https://www.bucap.it/news/approfondimenti-tematici/continuta-operativa/cloud-caratteristiche.htm>

Le informazioni sulle caratteristiche del cloud computing sono state raccolte da diverse fonti:

¹⁵ <https://www.guru99.com/characteristics-of-cloud-computing.html#multitenancy-and-resource-pooling>

¹⁶ <https://www.atlassian.com/it/microservices/cloud-computing>

¹⁷ https://www.ctmobi.it/cloud/cloud-computing-cose-come-funziona-e-perche-conviene/#Le_cinque_caratteristiche_essenziali_del_Cloud_Computing

¹⁸ <https://vitolvecchia.altavista.org/definizione-caratteristiche-principali-del-cloud-computing/>

¹⁹ Lezioni di organizzazione dei sistemi informativi dell'azienda del Professore Francesconi e di metodologie e tecniche dell'impresa digitale del Professore Del Vecchio

1. **Elasticità e scalabilità rapide** – Nel cloud computing gli utenti possono facilmente aumentare o diminuire le risorse di elaborazione in base alle loro esigenze e questo permette alle organizzazioni di adattarsi rapidamente ai cambiamenti del mercato e di gestire i picchi di domanda.

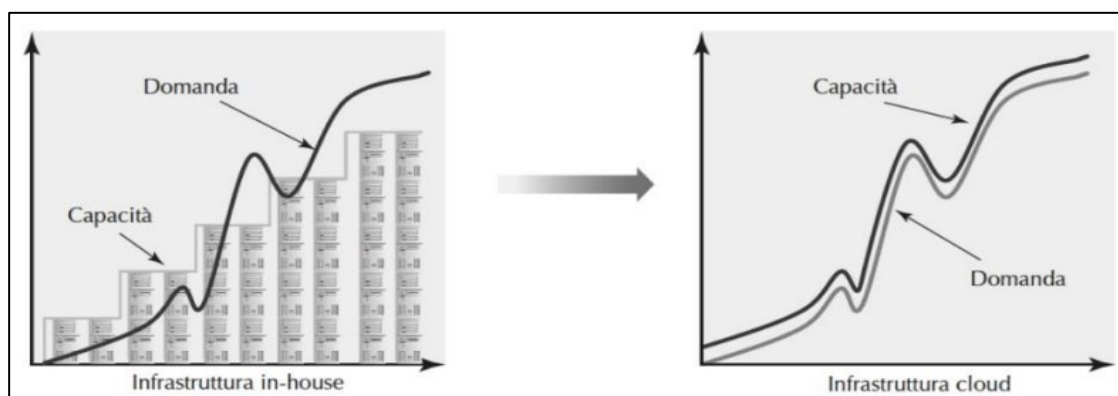


Figura 3 – Soddisfare i picchi di domanda con l'infrastruttura in sede e cloud

Con una struttura in-house è difficile soddisfare i picchi di domanda: se le esigenze di uso delle risorse ICT crescono rapidamente le aziende che hanno le risorse in casa difficilmente riescono a crescere in tempi rapidi.

Con una struttura cloud l'azienda attraverso un approccio incrementale e decrementale può avvicinarsi alla domanda di risorse informatiche senza prevedere a priori gli investimenti o le implementazioni.

Le risorse informatiche non vengono usate in maniera omogenea nel tempo: ci sono dei momenti di picco in cui le risorse vengono realmente sfruttate, e in questo caso l'investimento è ben sfruttato, e ci sono altri momenti (non di picco) dove l'investimento è considerato eccessivo rispetto alle esigenze in quanto le risorse non vengono sfruttate al 100%.

È difficile soddisfare perfettamente la domanda di risorse informatiche in tempi rapidi usando un'infrastruttura in-house, invece, con il cloud computing fornito dai service provider gli utilizzatori possono facilmente regolare l'ampiezza delle risorse informatiche (facendo scaling up and down) in base alle proprie esigenze, così da

adattarsi velocemente ai cambiamenti del mercato.

Dal punto di vista economico la flessibilità dell'azienda si traduce in sostituzione degli investimenti in risorse ICT, che sono costi fissi, in costi variabili. Modificando in questo modo la spesa dell'infrastruttura viene conferita all'azienda maggiore dinamicità.

2. **Automazione** – Il cloud computing permette agli utenti di richiedere e gestire le risorse di elaborazione in modo autonomo e immediato (senza richiedere l'intervento umano diretto). Questo offre agli utenti un controllo maggiore sulle loro risorse e permette loro di adattare rapidamente le risorse alle loro esigenze.
3. **Multi-tenancy e resource pooling** – Nel cloud computing, la multi-tenancy è “l'architettura software che permette a una singola istanza di programma di fornire servizi a più utenti finali. Questa caratteristica consente l'uso delle stesse risorse di calcolo da parte di più clienti”²⁰.
4. **Ampio accesso alla rete** – Il cloud computing si basa sulla connettività di rete. Questo significa che è possibile accedere ai servizi forniti dal service provider da qualsiasi luogo attraverso vari devices, purché abbiano una connessione a Internet. Per gli utenti si traduce in maggiore mobilità e autonomia, tuttavia, senza la rete i servizi cloud non possono funzionare. Il cloud computing promuove la caratteristica del lavoro remoto.
5. **Servizio misurato e segnalato** – Nel cloud computing, l'uso delle risorse è misurato con precisione. Questo permette agli utenti di monitorare e controllare i loro costi, e ai fornitori di cloud di offrire un modello di fatturazione basato sull'uso.
6. **Struttura di pagamento basato sull'uso** – Con il cloud computing, gli utenti pagano solo per le risorse che effettivamente utilizzano. Questo modello di “utility computing” può essere più economico rispetto all'acquisto e alla gestione delle proprie risorse informatiche.

²⁰ <https://www.ibm.com/it-it/topics/multi-tenant>

7. **Facile manutenzione** – Il cliente non è coinvolto nella gestione di problematiche di manutenzione né deve attivare contratti onerosi con società di consulenza per l'operatività e dell'utenze e del sistema. Infatti, nella configurazione del servizio cloud è previsto che sia il fornitore a gestire la manutenzione del tutto.
8. **Patch** – La gestione delle patch, in ottica cloud, consente alle imprese di avere sei servizi sempre aggiornati ²¹ e protetti rispetto a quelle che sono le potenziali minacce a cui il servizio è esposto. Seppur le fasi di gestione di una patch possono rivelarsi lunghe, queste si rendono necessarie al fine di consolidare il funzionamento e la conformità della tecnologia rilasciata ai clienti.
9. **Resilienza** – Il cloud computing offre un up-time del server continuo, e quindi offre servizi resilienti. Offre la capacità di recuperare da qualsiasi interruzione del servizio.
10. **Sicurezza per la protezione dei dati** – I principali fornitori di servizi cloud investono considerevolmente nella sicurezza delle loro infrastrutture e in molti casi le misure di sicurezza adottate dai maggiori provider si rivelano maggiori rispetto a quelle che la singola impresa riuscirebbe autonomamente ad implementare al proprio interno. Tuttavia, è importante considerare che la sicurezza nel cloud è una responsabilità condivisa: le aziende devono collaborare attivamente con i fornitori per garantire la protezione dei propri dati e delle proprie risorse. In alcuni settori vigono normative e standard di sicurezza rigidi e in queste situazioni i fornitori devono garantire che l'implementazione e l'utilizzo del cloud sia conforme a tali regole settoriali.

1.2 Principali modelli

Il concetto di "as-a-Service" può essere indicativo di un servizio di cloud computing gestito da un provider esterno per conto di uno specifico utente, permettendogli di concentrarsi sulle

²¹ <https://www.securityopenlab.it/news/2254/le-5-best-practice-per-gestire-al-meglio-le-patch-di-sicurezza-dei-workload-cloud.html>

attività strategiche. Ogni forma di cloud computing offre la possibilità di affidare la gestione di un numero crescente di componenti dell'infrastruttura on-premise, eliminando la necessità di "acquistare, gestire o utilizzare hardware, software, strumenti o applicazioni da un data center on-premise" ²².

È possibile quindi, seguendo tale concezione, accedere ai servizi on demand attraverso una connessione internet sottoscrivendo un abbonamento o pagandolo in base al consumo ²³.

Se invece si vuole analizzare la tipologia di infrastruttura IT on-premise, questa implica un alto grado di responsabilità gestionale poiché tutte le attività di gestione, aggiornamento, manutenzione e sostituzione degli hardware e software ospitati localmente sono di competenza dell'azienda e del suo team IT, richiedendo a questa quindi un impegno di risorse dedicate nella gestione del tutto.

Il cloud computing, al contrario, offre un'alternativa flessibile che può ridurre significativamente il carico di gestione IT, così da lasciare spazio e tempo per dedicarsi ad altre attività di tipo strategiche e/o per favorire un livello della struttura dei costi più sostenuto. A seconda del modello di servizio cloud scelto (SaaS, PaaS o IaaS), è possibile delegare la gestione di uno, alcuni o tutti i componenti dell'infrastruttura IT a un fornitore di servizi cloud.

Esistono tre principali categorie di cloud computing as-a-Service, ognuna con un diverso grado di gestione lasciata all'utente:

- Software-as-a-Service (SaaS),
- Infrastructure-as-a-Service (IaaS),
- e Platform-as-a-Service (PaaS) ²⁴.

²² <https://cloud.google.com/learn/paas-vs-iaas-vs-saas?hl=it>

²³ <https://www.redhat.com/it/topics/cloud-computing/iaas-vs-paas-vs-saas>

²⁴ <https://injenia.it/inthinking/iaas-paas-saas-quali-differenze/>

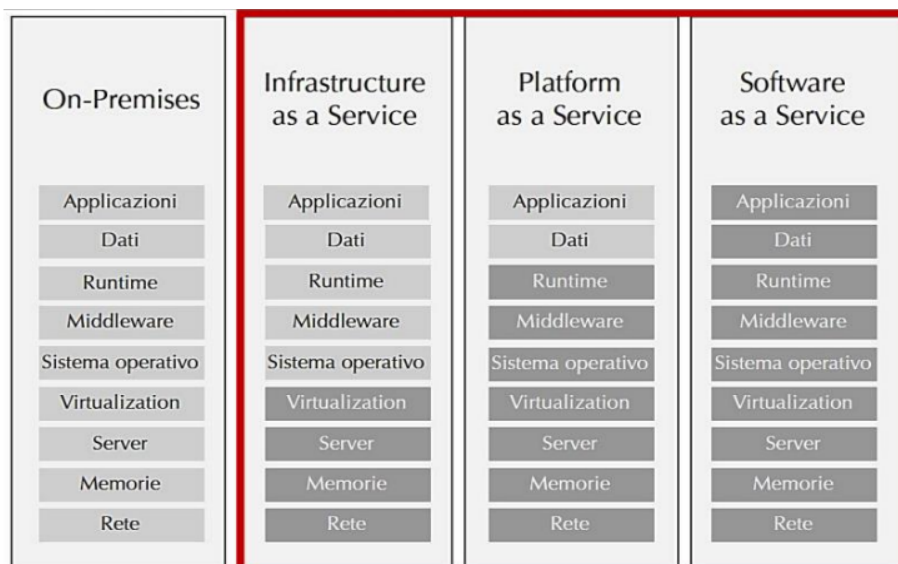


Figura 4 – Nella tabella è raffigurata la soluzione On-premises e quella Cloud computing evidenziando la differenza in termini di controllo: in grigio chiaro gli elementi gestiti internamente e in grigio scuro ciò che è gestito da terzi ²⁵

1.2.1 Software as a service – SaaS (Cloud applications)

Per Red Hat, la concezione di SaaS nota anche come servizi applicativi cloud, è la tipologia più completa di servizi in ambito cloud computing, la quale consiste nella fornitura di un'intera applicazione gestita da un provider per tramite di un browser web ²⁶. Il servizio offerto consiste in un'applicazione software che è installata nei server del fornitore e gli utenti possono accedervi da remoto. Questo approccio è adatto per chi vuole ridurre al massimo la gestione di software, server e aggiornamenti. Infatti, tramite questo servizio l'utente può utilizzare un applicativo senza doversi preoccupare di gestire i dettagli tecnici come hardware, infrastruttura di rete o sistema operativo ²⁷.

“Gmail”, “Dropbox”, “Office 365” e “Salesforce” sono solo alcuni esempi di servizi SaaS ²⁸.

²⁵ Lezioni di organizzazione dei sistemi informativi dell'azienda del Professore Francesconi

²⁶ <https://www.redhat.com/it/topics/cloud-computing/iaas-vs-paas-vs-saas>

²⁷ Faggioli, G., & Italiano, A. (2017). *I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider*. Franco Angeli.

²⁸ Lezioni di metodologie e tecniche dell'impresa digitale del Professore Del Vecchio

1.2.2 Platform as a service – PaaS (Cloud platforms)

Secondo IBM “Platform-as-a-Service, o PaaS, fornisce una piattaforma cloud per lo sviluppo, l'esecuzione e la gestione di applicazioni” ²⁹.

In questo caso il provider mette a disposizione una piattaforma sulla quale il cliente realizza le sue applicazioni ³⁰. Questo servizio è conveniente per gli sviluppatori in quanto abilita loro ad utilizzare l'ambiente di hosting per le loro applicazioni mantenendo il controllo su tutti gli elementi presenti.

Il provider si occupa invece del sistema operativo, dell'hardware e dell'infrastruttura di rete. A differenza di SaaS, PaaS offre un livello di autonomia maggiore, consentendo all'azienda cliente di gestire le applicazioni nell'ambiente di hosting.

Tra le soluzioni PaaS vi sono: “Google App Engine” e “Microsoft Azure Services” ³¹.

1.2.3 Infrastructure as a service – IaaS (Cloud infrastructure)

Secondo Google il modello Infrastructure as a Service (IaaS) offre alle organizzazioni risorse di infrastruttura on demand tramite il cloud, quali ad esempio capacità di calcolo, spazio di archiviazione, networking e virtualizzazione. I clienti non devono preoccuparsi della gestione, della manutenzione o degli aggiornamenti della propria infrastruttura di data center, ma sono responsabili del sistema operativo, del middleware, delle macchine virtuali e di qualsiasi applicazione o dato ³².

Questo modello è adatto per le imprese che hanno esigenze specifiche di configurazione e gestione dei server, poiché fornisce un controllo completo sull'infrastruttura, sul sistema operativo, sull'hardware e sulla rete ^{33 34}.

Ad esempio, i fornitori di servizi IaaS sono: “Amazon Web Services”, “Oracle”, “IBM” e “Compute Engine di Google Cloud Platform”.

²⁹ <https://www.ibm.com/it-it/topics/iaas-paas-saas>

³⁰ Faggioli, G., & Italiano, A. (2017). *I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider*. Franco Angeli.

³¹ Lezioni di metodologie e tecniche dell'impresa digitale del Professore Del Vecchio

³² <https://cloud.google.com/learn/paas-vs-iaas-vs-saas?hl=it>

³³ [Cos'è il modello IaaS? Infrastructure as a Service, Infrastruttura distribuita come servizio | Microsoft Azure](#)

³⁴ [Cos'è una soluzione IaaS \(Infrastructure-as-a-Service\)? | IBM](#)

1.2.4 Hybrid (Multi-cloud)

È possibile anche considerare una soluzione Hybrid, o Multi-cloud: l'azienda può decidere di non limitarsi scegliendo solo la soluzione On-premise o solo quella Cloud ma può pensare di combinarle per soddisfare diverse esigenze all'interno della tua organizzazione. Così facendo l'azienda può decidere di mantenere il controllo su determinati dati, mantenendoli nella propria infrastruttura, e per altri aspetti può affidarsi al cloud per aumentare la sua flessibilità³⁵.

1.3 Principali modalità di distribuzione

Come già accennato nei paragrafi precedenti, il cloud computing consente l'abilitazione ai clienti che ne fanno richiesta di specifiche risorse, attraverso il semplice utilizzo di internet³⁶. Queste risorse possono essere distribuite in diverse modalità, ciascuna con le sue specifiche caratteristiche e vantaggi. Le principali modalità di distribuzione sono:

- Public Cloud,
- Private Cloud,
- Community Cloud
- e Hybrid Cloud.

³⁵ Lezioni di organizzazione dei sistemi informativi dell'azienda del Professore Francesconi e di metodologie e tecniche dell'impresa digitale del Professore Del Vecchio

³⁶ [https://www.ibm.com/it-it/topics/cloud-computing#:~:text=Il%20cloud%20computing%20%C3%A8%20un,servizi%20cloud%20\(o%20CSP\)](https://www.ibm.com/it-it/topics/cloud-computing#:~:text=Il%20cloud%20computing%20%C3%A8%20un,servizi%20cloud%20(o%20CSP))

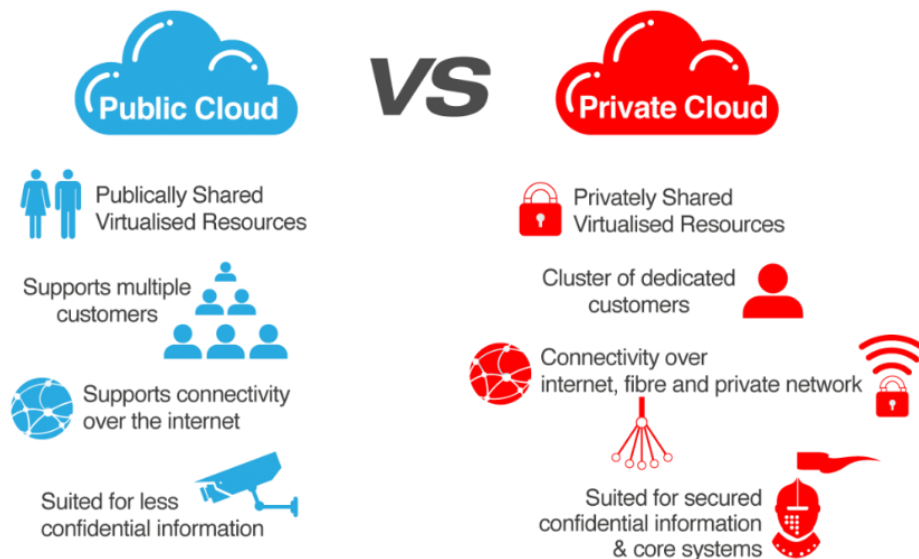


Figure 5 - Cloud pubblico e cloud privato: quali sono le differenze? ³⁷

1.3.1 Public Cloud

Secondo Microsoft, il cloud pubblico è costituito da servizi di elaborazione forniti da fornitori esterni tramite la rete internet pubblica e accessibili a chiunque ne abbia bisogno o desideri acquistarli. Questi servizi possono essere gratuiti o venduti su richiesta, consentendo ai clienti di pagare solo per le risorse di calcolo, archiviazione o larghezza di banda utilizzate ³⁸.

In base alla definizione del Gruppo di Lavoro ex art. 29 dir. 95/46/CE2, il Public Cloud è quel modello dove l'infrastruttura è amministrata da un fornitore specializzato nella fornitura di servizi, il quale offre i propri sistemi agli utenti, alle aziende o alle pubbliche amministrazioni, condividendoli tra di loro ³⁹.

Praticamente, gli ambienti del Cloud Pubblico sono implementati su un'infrastruttura IT di proprietà del provider, suddivisa e ridistribuita su più mandanti (utenti provenienti da diverse organizzazioni). Questa tipologia di struttura è definita come multi-tenant e/o multi-mandante, dove viene espressamente indicato che gli utenti condividono l'utilizzo

³⁷ <https://nds.id/en/public-cloud-en/>

³⁸ [Che cos'è un cloud pubblico - Definizione | Microsoft Azure](#)

³⁹ Faggioli, G., & Italiano, A. (2017). *I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider*. Franco Angeli.

dell'infrastruttura, e dei servizi ad essa collegati ^{40 41}.

I Cloud Pubblici, a differenza dei Cloud Privati, permettono alle aziende di ottenere un risparmio sui costi relativi all'acquisto, alla gestione e alla manutenzione di un'infrastruttura locale per applicazioni e hardware, poiché il provider cloud si assume la responsabilità di tutte le operazioni di gestione e manutenzione. Inoltre, i Cloud Pubblici offrono una piattaforma scalabile e possono essere distribuiti più rapidamente rispetto alle infrastrutture locali. La connettività a Internet consente a tutti i dipendenti di accedere alle stesse applicazioni da qualsiasi dispositivo. Nonostante gli ambienti Cloud Pubblico possano sollevare alcune preoccupazioni in merito alla sicurezza degli stessi, se implementati correttamente, può essere comunque garantito lo stesso livello di sicurezza del cloud privato ⁴².

Secondo le ultime previsioni di Gartner, la spesa mondiale degli utenti finali per i servizi Cloud Pubblici è cresciuta del 21,7%, raggiungendo un totale di 597,3 miliardi di dollari nel 2023, rispetto ai 491 miliardi di dollari del 2022 ⁴³.

1.3.2 Private Cloud

L'organizzazione che utilizza l'infrastruttura cloud è la sola proprietaria e detiene il completo controllo su di essa ⁴⁴, pertanto, di conseguenza in un cloud privato non vi è la condivisione delle risorse con altre società di cloud computing.

Numerose aziende preferiscono l'utilizzo di cloud privato rispetto al cloud pubblico al fine di rispettare gli standard di conformità normativa o per gestire in maniera appropriata le informazioni sensibili quali documenti confidenziali, proprietà intellettuale, dati personali, registrazioni mediche e informazioni finanziarie. Il cloud privato consente una gestione accurata della privacy e della sicurezza dei dati, permettendo l'accesso alle risorse condivise solo ai membri autorizzati dell'organizzazione.

Tipicamente, un cloud privato risiede in modalità on-premise nel data center del cliente.

⁴⁰ <https://www.redhat.com/it/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud>

⁴¹ <https://www.ibm.com/it-it/topics/public-cloud>

⁴² [Che cos'è un cloud pubblico - Definizione | Microsoft Azure](#)

⁴³ <https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023>

⁴⁴ Faggioli, G., & Italiano, A. (2017). *I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider*. Franco Angeli.

Inoltre, questo può essere installato su un'infrastruttura indipendente del provider del cloud oppure può essere implementato su un'infrastruttura affittata che si trova in un data center esterno ⁴⁵.

Lo svantaggio è che la gestione del cloud privato spetta al reparto IT dell'azienda. Di conseguenza i costi relativi al personale, alla gestione e alla manutenzione dei data center di proprietà tradizionali (previsti dalla soluzione on-premise) sono gli stessi per i cloud privati ⁴⁶.

1.3.3 Community Cloud

“Un community cloud (cloud comunitario) è un'infrastruttura cloud in cui più organizzazioni condividono risorse e servizi in base a requisiti operativi e normativi comuni” ⁴⁷.

Il mercato del cloud comunitario è una branca specializzata del cloud computing dedicata a soddisfare le esigenze di una specifica comunità o gruppo di organizzazioni. A differenza dei cloud pubblici, aperti a tutti gli utenti, i cloud comunitari sono progettati per un numero limitato di utenti con esigenze simili. Questi forniscono una soluzione su misura per ciascun membro della comunità, condividendo infrastruttura, risorse e servizi. Ciò facilita la cooperazione, la condivisione di dati e applicazioni, nonché benefici economici derivanti dalle economie di scala. I cloud comunitari spesso servono settori come la sanità, la pubblica amministrazione, la finanza o l'istruzione, che hanno specifici requisiti normativi ⁴⁸.

In pratica, un'unica infrastruttura cloud è fornita da un fornitore a un gruppo ristretto di organizzazioni utenti che solitamente condividono la stessa missione aziendale o gli stessi requisiti di business. Di conseguenza, queste organizzazioni richiedono che il servizio offerto rispetti specifiche caratteristiche come i livelli di sicurezza, la riservatezza dei dati e la conformità alle normative di settore ⁴⁹.

Come visto, il cloud pubblico e quello privato sono le principali tipologie di implementazione

⁴⁵ [Cos'è il cloud computing? | IBM](#)

⁴⁶ [Che cos'è un cloud privato - Definizione | Microsoft Azure](#)

⁴⁷ <https://www.spiceworks.com/tech/cloud/articles/what-is-community-cloud/>

⁴⁸ [Rapporto sul mercato del cloud comunitario | Analisi e previsioni - 2032 \(alliedmarketresearch.com\)](#)

⁴⁹ Faggioli, G., & Italiano, A. (2017). *I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider*. Franco Angeli.

favorite nel mercato, anche la domanda di cloud comunitario è in crescita. Secondo un rapporto di Allied Market Research, il mercato globale del cloud comunitario era valutato a \$4.7 miliardi nel 2022, e si prevede che raggiungerà \$82.9 miliardi entro il 2032, crescendo a un tasso di crescita annuo composto (CAGR) del 33.6% dal 2023 al 2032 ⁵⁰.

1.3.4 Hybrid Cloud

Il cloud ibrido combina ambienti di cloud pubblico e cloud privato ^{51 52 53}.

- Nel cloud pubblico, le risorse sono gestite da un provider di servizi cloud terzo e sono condivise tra vari clienti. Questo offre una grande scalabilità e riduce i costi, poiché si paga solo per le risorse utilizzate.
- Il cloud privato, d'altra parte, è dedicato a un'organizzazione singola. Offre un controllo maggiore sulle risorse e sulla sicurezza, il che è particolarmente utile per le aziende con requisiti di conformità rigorosi.

Unendo questi due ambienti un'azienda può sfruttare il meglio di entrambi i mondi. Ad esempio, potrebbe utilizzare il cloud privato per dati sensibili, mentre sfrutta il cloud pubblico per le applicazioni non critiche o per gestire picchi di carico di lavoro.

Molte aziende stanno implementando una strategia cloud ibrida. Secondo un rapporto di Mordor Intelligence, si prevede che il mercato globale delle soluzioni di cloud ibrido crescerà a un tasso di crescita annuo composto (CAGR) del 22,12% nel periodo di previsione 2024 - 2029. La dimensione del mercato del cloud ibrido è stimata in USD 129,68 miliardi nel 2024 e si prevede che raggiungerà USD 352,28 miliardi entro il 2029 ⁵⁴.

Anche in Italia, il mercato del cloud computing è in forte crescita. Secondo l'Osservatorio Cloud Transformation, nel 2023 il mercato del cloud, nello scenario italiano, aveva un valore di 5,51 miliardi di euro, con un aumento del 19% rispetto al 2022. La componente di Public & Hybrid Cloud ha dimostrato una crescita più rilevante, con una spesa di 3,729 miliardi di

⁵⁰ [Community Cloud Market Report | Analysis & Forecast - 2032 \(alliedmarketresearch.com\)](https://www.alliedmarketresearch.com/community-cloud-market-report-analysis-forecast-2032)

Le informazioni sulle caratteristiche del hybrid cloud sono state raccolte da diverse fonti:

⁵¹ [Cos'è il cloud ibrido e qual è il significato di ambiente cloud? | Cloudflare](https://www.cloudflare.com/learning/cloud/what-is-hybrid-cloud/)

⁵² [Che cos'è il cloud ibrido? - Vantaggi e svantaggi di un cloud ibrido | NetApp](https://www.netapp.com/resources/whitepapers/what-is-hybrid-cloud/)

⁵³ [Cloud Ibrido: cosa è ed i vantaggi - IWS Consulting](https://www.iwsconsulting.com/it/cloud-ibrido-cosa-e-ed-i-vantaggi/)

⁵⁴ <https://www.mordorintelligence.com/industry-reports/hybrid-cloud-market>

euro, in aumento del 24% rispetto al 2022 ⁵⁵. In un sondaggio condotto tra i responsabili IT, il 58% ha affermato di utilizzare una strategia ibrida cloud, rispetto al 51% dell'anno precedente (*Fonte: Fondazione Cloud*) ⁵⁶.

Questo, è un chiaro segnale di come si stia assistendo ad un allineamento tra la crescita del mercato del cloud e l'adozione di strategie ibride cloud da parte delle aziende in Italia.

Il cloud ibrido e il multi-cloud sono due approcci distinti alla gestione delle risorse cloud, ognuno con i suoi vantaggi ^{57 58}:

- **Il cloud ibrido combina l'uso di risorse cloud pubbliche e private** per eseguire la stessa attività. Questo approccio consente alle aziende di sfruttare i vantaggi di entrambi i tipi di cloud, come la sicurezza e il controllo dei cloud privati e la scalabilità e l'accessibilità dei cloud pubblici. Uno degli obiettivi del cloud ibrido è quello di eliminare la dipendenza da un singolo provider di servizi cloud e di rispettare i requisiti normativi.
- D'altra parte, **un approccio multi-cloud implica l'utilizzo di servizi da più provider di cloud pubblici** per eseguire diverse attività (i servizi dei diversi cloud pubblici sono gestiti in modo separato). Questo può offrire, ad esempio, una maggiore resilienza, poiché in questo caso le aziende utenti non sono legate a un singolo provider di servizi cloud.

Un ambiente cloud ibrido può essere considerato multi-cloud se utilizza risorse da un cloud privato e da almeno due provider di servizi cloud pubblici. Tuttavia, la chiave per un vero ambiente cloud ibrido è l'integrazione e l'interoperabilità tra i diversi ambienti cloud.

⁵⁵ [Mercato Cloud Computing in Italia in crescita del 19% \(osservatori.net\)](#)

⁵⁶ <https://www.lambertconsulting.ch/it/statistiques-et-tendances-du-cloud-computing-2023-2024/>

Le informazioni sulle caratteristiche del multi-cloud sono state raccolte da diverse fonti:

⁵⁷ <https://www.vmware.com/it/topics/glossary/content/multi-cloud-strategy.html>

⁵⁸ <https://cloud.google.com/learn/what-is-hybrid-cloud?hl=it>

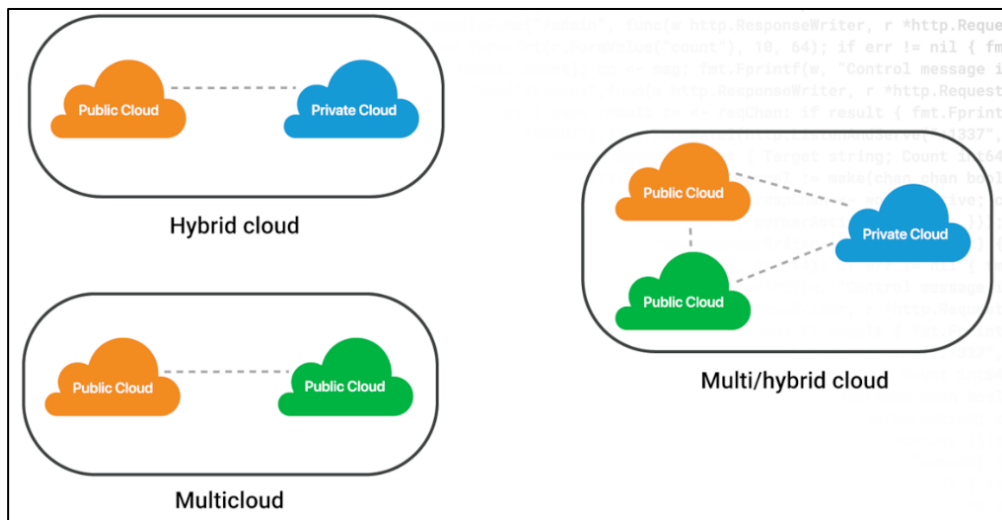


Figura 5 - Rappresentazione del Cloud ibrido e del Multi-cloud ⁵⁹

1.4 Problematiche del cloud computing

Secondo Google Cloud, gli svantaggi che possono emergere nell'adozione di tecnologia cloud computing, possono essere svariati ⁶⁰. In primis, basti pensare che è una tecnologia basata prevalentemente sull'utilizzo di internet, il quale può sembrar scontato, ma è necessario che la connessione sia solida e cablata in quanto, questo aspetto, impatta su quelli che sono i servizi a cui si può accedere. Avere dei problemi di connessione può voler implicare un accesso minore ai servizi cloud generando così insoddisfazione per il cliente.

Inoltre, oltre a questo aspetto generale, è possibile comunque individuare in cluster quelle che sono le problematiche del cloud ⁶¹:

- Rischio di vincoli al fornitore
- Un minor controllo sull'infrastruttura cloud sottostante
- Preoccupazioni relative a rischi per la sicurezza quali privacy dei dati e minacce online

⁵⁹ <https://www.akamai.com/it/glossary/what-is-hybrid-cloud>

⁶⁰ <https://cloud.google.com/learn/advantages-of-cloud-computing?hl=it>

⁶¹ Ibidem.

- Complessità di integrazione con i sistemi esistenti
- Costi e spese imprevisti

Per effettuare una buona mitigazione di questi rischi è necessario selezionare al meglio il sistema di offerta di un fornitore al fine di valutare se, nella sua value proposition, possa coprire uno o più rischi in modo da vincolarsi a delle clausole contrattuali che possano garantire una maggior tutela.

Di seguito, si tratteranno nel dettaglio alcune delle problematiche più ostiche.

1.4.1 Residenza dei dati e compliance

La gestione dei dati sensibili è un tema fortemente sentito nell'epoca attuale tanto che, le imprese, sono tenute ad osservare rigide regole di gestione degli stessi. Rispetto a quello che è l'utilizzo del cloud computing, nonostante i notevoli vantaggi in termini di velocità e riduzione dei costi, già accennati nella trattazione, vi è anche la necessità di una gestione accurata della conformità al Regolamento generale sulla protezione dei dati (GDPR) ⁶².

La complessità della conformità è accentuata dalla minore visibilità sul ciclo di vita dei dati rispetto alle soluzioni on-premise e dalla necessità di stipulare accordi contrattuali con i fornitori di servizi cloud per garantire la corretta gestione e protezione dei dati. Per far fronte a ciò è necessario prestare attenzione a quanto richiesto dal GDPR in termini di responsabilità del titolare nel trattamento dei dati.

Secondo l'articolo 28 del GDPR ⁶³, il titolare deve scegliere esclusivamente responsabili del trattamento che possano fornire adeguate garanzie e misure tecniche/organizzative al fine di assicurare la conformità alle normative e proteggere i diritti degli interessati. Inoltre, l'articolo 28 richiede che i trattamenti effettuati da un responsabile del trattamento siano rigorosamente disciplinati da contratti che adempiano a quelli che sono i requisiti normativi.

In questo scenario, il Cloud Provider, in qualità di responsabile esterno, può essere chiamato a rispondere per intero per i danni causati agli interessati se non rispetta gli obblighi

⁶² <https://www.cybersecurity360.it/legal/privacy-dati-personali/servizi-cloud-e-compliance-gdpr-obblighi-e-soluzioni/>

⁶³ <https://www.privacy-regulation.eu/it/28.htm>

contrattuali con il titolare o viola le disposizioni del GDPR relative ai responsabili del trattamento.

1.4.1.1 Valutare dati da esternalizzare

Nella valutazione sulla gestione dei dati, la figura del Cloud Provider risulta essere chiave. Per capire al meglio ciò, è necessario fare un parallelo tra quella che è la gestione dei dati in un sistema on premise verso un sistema cloud ⁶⁴.

Nel sistema cloud, i dati vengono gestiti, memorizzati ed archiviati attraverso tecnologie messe a disposizione dal provider, dando così dei vantaggi in termini di elasticità dell'infrastruttura mentre, nei servizi on premise, i dati sono gestiti localmente in locali e/o strutture gestite internamente dalle aziende. Questo, come già accennato precedentemente, comporta rigidità ed un aumento della struttura dei costi interni dell'azienda.

Entrambi gli approcci offrono comunque dei vantaggi ma, dietro di questi, vi è necessità di stabilire un processo decisionale in modo da valutare quelli che sono i dati da esternalizzare. Tale processo, può comportare anche allo stabilire di una politica mista ⁶⁵ di gestione dei dati, la quale può essere frutto di valutazione dei seguenti fattori ⁶⁶:

- 1. Sensibilità dei dati:** i dati sensibili possono riguardare alcune informazioni relative ai clienti quali indirizzo, IBAN ed altre simili. Per tale motivo, la necessità di sicurezza in questi casi è maggiore ed è preferibile adottare strumenti di sicurezza interni piuttosto che esternalizzare tali informazioni in un cloud.
- 2. Requisiti Normativi:** sull'aspetto normativo, è necessario che la gestione si adegui a quelle che sono le specifiche richieste di settore infatti, ad esempio, un'azienda che opera nel settore sanitario potrebbe essere soggetta a norme più stringenti e, pertanto, è possibile scegliere una soluzione cloud ma che rispetti i vincoli normativi.

⁶⁴ Garante per la protezione dei dati, "Cloud computing: indicazioni per l'utilizzo consapevole dei servizi", pag. 9 e ss, consultabile al <https://www.garanteprivacy.it/documents/10160/10704/1819933>

⁶⁵ <https://cloud.google.com/learn/what-is-cloud-data-security?hl=it>

⁶⁶ Ibidem

3. **Flessibilità e scalabilità:** se l'azienda ha necessità di gestire picchi di lavoro temporanei, così come già discusso precedentemente, ricorrere alla soluzione cloud consente una più ampia flessibilità nella gestione dei dati.
4. **Perdita di controllo:** poiché i dati e le applicazioni risiedono su un'infrastruttura gestita da terze parti, le aziende hanno una minore capacità di controllare come i dati vengono accessi e condivisi.
5. **Costi:** infine, come per gli altri aspetti legati al cloud computing, anche i costi sono da valutare in quanto scegliere un paniere di dati da esternalizzare comporta la scelta di provider ed il sostenimento di costi di licenze e archiviazione che devono essere necessariamente soppesati rispetto ad una gestione interna degli stessi.

1.4.2 Lock in

Il Lock-in è un altro aspetto da tener conto nella scelta di un servizio cloud. Nel settore dei servizi ICT, il termine, ha un'accezione legata al fatto che spesso un cliente ha più o meno manovra nella selezione dei propri fornitori. Qualora l'amministrazione risulti non essere in grado di cambiare facilmente fornitore al termine del periodo contrattuale, può incorrere a problematiche relative alle informazioni da quest'ultimo gestite ⁶⁷. In effetti più il fornitore possiede elementi unici e indispensabili, di cui è l'unico custode, più diventa difficile allentare questo vincolo. Sia che si tratti di informazioni esclusive e riservate, sia di componenti sviluppati su misura, è evidente che il rapporto tra fornitore e cliente è fortemente sbilanciato a favore del primo. Questo consente al fornitore di imporre più facilmente modifiche contrattuali, preventivi o ricambi, sapendo che per il cliente sarebbe difficile e probabilmente costoso cambiare fornitore.

Nello scenario dei servizi cloud ⁶⁸, queste situazioni, possono essere scongiurate attraverso l'applicazione di determinati contratti e, relative clausole, che possano vincolare i fornitori uscenti a supporto verso il cliente di quella che nel gergo viene definita data migration ⁶⁹

⁶⁷ <https://www.aruba.it/magazine/cloud/lock-in-come-evitarlo-e-come-uscirne-con-successo.aspx>

⁶⁸ Ibidem.

⁶⁹ <https://magazine.wiit.cloud/cloud-as-a-service-le-4-criticita0-pi0C3%B9-sottovalutate-e-come-risolverle>

ovvero la messa a disposizione di disponibilità, effort, competenze e strumenti atti a trasferire i dati da una piattaforma all'altra in modo da ridurre gli impatti del change di fornitura.

1.4.3 Servizi standard

Infine, e non per importanza, è necessario menzionare i servizi standard che vengono erogati attraverso il cloud computing. Di solito ⁷⁰, i servizi cloud sono presentati come insiemi di offerte standardizzate, progettate per consentire un'attivazione agevole e sistematica dei servizi stessi. Questi servizi sono in grado di adattarsi alle variazioni di carico, aumentando o diminuendo risorse in modo trasparente e automatico durante i picchi di utilizzo. Tutto ciò avviene in modo sicuro, permettendo ai diversi utenti di operare contemporaneamente sui propri dati e sistemi.

Pertanto, la configurazione dello stesso servizio è predeterminata rendendo limitata la possibilità di applicare delle change request utili a customizzare il tutto in base a quelle che sono le esigenze del cliente. Inoltre, essendo la gestione della piattaforma nelle mani del provider, è possibile che, qualora questi adotti delle proprie politiche di upgrade dei suoi sistemi, il cliente non abbia altra strada che adeguarsi senza possibilità di resistenza.

⁷⁰ https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/2_il_cloud_computing.html

Capitolo 2 - Confronto contrattuale tra Modello Classico e Cloud Computing

2.1 Modello classico per realizzare sistema informativo

Come già sottolineato nel capitolo precedente, il ricorso alle tecnologie di cloud computing sta diventando, e senz'altro lo diventerà sempre più, protagonista tra imprese IT e PA. La sua importanza non può prescindere, però, dal delineare anche alcuni punti critici che verranno trattati nelle prossime pagine, e un confronto strutturale con quello che a tutti gli effetti può essere definito come un modello classico di contrattualistica.

In forma generale, i contratti ad oggetto informatico sono tutti quei contratti legati o a servizi informatici o che riguardano la creazione/gestione di beni quali hardware e software. Di fatti, un'azienda si troverà nella condizione di sottoscrivere un contratto sia per lo sviluppo di un nuovo sistema informativo ma anche per la gestione di uno già esistente.

Tali contratti, che possono rientrare in un modello classico, hanno una serie di caratteristiche ben specifiche che lo differenziano dai contratti di cloud computing.

2.1.1 Molteplici contratti

Una prima fondamentale caratteristica è quella riguardante la necessità di stipulare più contratti in riferimento alle varie esigenze e ai vari terreni di operatività (chiaramente non è detto che vengano redatti tutti indistintamente):

- **Contratto di licenza d'uso software:** tale contratto viene stipulato in quanto in esso vengono stabiliti termini e condizioni di utilizzo del software. È bene chiarire che in questa tipologia di contratti, il cliente / utente non acquisisce il diritto di proprietà del software bensì il diritto di godimento, non esclusivo, dello stesso secondo un determinato e vincolante periodo di tempo, ben specificato in esso, e in cambio di una certa somma concordata dalle parti. Un'altra implicazione da considerare è quella legata alle garanzie negoziali e alla responsabilità del fornitore: è, infatti, usuale che

nei contratti di licenza d'uso vengano inserite non poche clausole per deresponsabilizzare il fornitore in caso di perdita di dati derivanti dall'utilizzo del software o anche eventualmente limitare un eventuale risarcimento danni ⁷¹.

Le imprese informatiche tendono a creare le loro offerte in modo da rendere il contratto di licenza d'uso particolarmente snello e per rendere quasi obbligatoria la stipula di un successivo contratto di manutenzione.

- **Contratto di manutenzione delle licenze:** nella gran parte dei casi, al contratto di licenza d'uso è poi legato uno di manutenzione. Tali contratti sono particolarmente importanti in quanto consentono al cliente di usufruire di supporto e aggiornamento del software che, in alcuni casi, è imprescindibile per il buon funzionamento ma anche di avvalersi di eventuali correzioni: questo perché i contratti di licenza molto spesso sono particolarmente restrittivi in merito a garanzie sul funzionamento e, come già esplicitato, tendono a ridurre al minimo il grado di responsabilità da parte del fornitore. È il caso di tutti quei programmi che vengono utilizzati per l'elaborazione di paghe e contributi, per tutti quei software legati alla contabilità di un'organizzazione, che devono necessariamente seguire e rispettare l'adeguamento delle normative a essi legati ed è per questo che necessitano di costante aggiornamento ⁷².

- **Contratto di approvvigionamento hardware,** che rientra nelle casistiche della compravendita o della locazione, in base alla natura della proprietà dell'hardware e al trasferimento del rischio.

Partendo dalla compravendita, un contratto di approvvigionamento hardware è tale se, in fase di negoziazione e stipula, le due parti coinvolte si accordano sul trasferimento del bene (quindi dal fornitore al cliente) in cambio di un prezzo previamente concordato. È chiaro, quindi, che in questo caso il fornitore trasferisce il diritto di proprietà sul bene e tutti gli aspetti, relativi ad esempio al trasferimento del rischio sul bene, sulla consegna o sulle garanzie di funzionalità, rientrano nella macro-casistica dei contratti di compravendita.

⁷¹ Farina M., (2018), I contratti informatici, Editore Key, pp.65-67

⁷² La manutenzione del software: clausole commentate, Camera di commercio industria artigianato e agricoltura di Torino, pp.8-9

Ma è anche possibile che tale tipologia di contratto hardware rientri nella locazione e quindi in una sorta di noleggio dell'hardware che il proprietario mette a disposizione. Diversamente dalla compravendita, il fornitore non perde la proprietà del bene e stabilisce in quali condizioni l'hardware deve essere utilizzato in cambio del pagamento di un canone. In tale tipologia di contratto rientrano tutte le caratteristiche di un contratto di locazione di beni mobili e può essere considerato come un contratto a prestazione continuativa ⁷³.

- **Contratto di implementazione:** un'altra tipologia di contratto che può essere stipulata riguarda l'implementazione *ex novo* di un software che rispetti le esigenze specifiche di un cliente. Si parla, quindi, non dell'installazione di un programma standard già esistente e quindi successivamente solo da personalizzare, ma di un processo più ampio che integra al tempo stesso sia la fase di fattibilità delle esigenze (di raccolta requisiti e analisi degli scopi del customer) e successivamente la fase di progettazione vera e propria. In casi di progetti molto dispendiosi, sia dal punto di vista economico sia dal punto di vista temporale, potrebbe essere usuale redigere due diversi contratti relativi ai due momenti sopracitati: in questo caso, è anche comune affidare a due diversi fornitori la fase di analisi e quella di implementazione.

Relativamente alla tipologia di contratto, andrà considerato anche il soggetto incaricato dello sviluppo: in caso si tratti di un imprenditore come nel caso di società di consulenza, il contratto assumerà la forma di contratto di appalto di servizi mentre se si tratta di un professionista e si parlerà di un contratto d'opera. Le attività e lo scopo saranno sostanzialmente identiche ma ciò che differisce è sul regime di responsabilità del fornitore ⁷⁴.

- **Contratto di assistenza e manutenzione:** tale contratto viene solitamente stipulato per un contesto di post go-live. Una volta che il progetto implementato superi positivamente la fase di test (UAT), è piuttosto tipico che il cliente decida di sottoscrivere un contratto che preveda assistenza e manutenzione: tale accordo

⁷³ Iaselli M., (2019). Lezioni di informativa giuridica, Key Editore

⁷⁴ Iaselli M., (2019). Lezioni di informativa giuridica, Key Editore,

disciplina non solo la possibilità per il fornitore di risolvere eventuali bug di programma ma anche di attivare prestazioni migliorative del programma stesso. Questo vale anche in caso di contratti di assistenza e manutenzione stipulati in caso di licenza d'uso software.

- Eventuale **contratto di outsourcing**: il contratto di outsourcing viene spesso sottoscritto dal cliente per affidare all'azienda fornitrice parte dei suoi processi aziendali o sistemi in approvvigionamento esterno. Basandosi sul servizio offerto, in materia di contratti di outsourcing, è possibile distinguere tra IT Outsourcing (ITO) e Business Process Outsourcing (BPO). L'ITO che fa riferimento proprio all'affidamento ad un fornitore esterno del proprio sistema applicativo ma anche delle infrastrutture tecnologiche, e quindi sia del software che dell'hardware, mentre il BPO è prevalentemente legato alla gestione a terzi di processi aziendali, come la parte amministrativa, logistica o di contabilità ⁷⁵.

È importante considerare che l'eventuale stesura di più contratti è possibile ed avviene in più momenti di negoziazione tra le parti. Infatti, un'altra importante caratteristica di questo modello contrattuale "classico" è proprio la possibilità di aprire più tavoli di comunicazione e momenti di negoziazione spalmati durante il progetto:

- **Sede precontrattuale**: una prima negoziazione avviene in una fase precontrattuale, all'inizio effettivo delle trattative. In questa prima fase, entrambe le parti potranno prepararsi su quelli che sono gli obiettivi da realizzare, priorità ed eventuali strategie da attivare: può essere un esempio quello di partire con proposte piuttosto rigide proprio per lasciare un margine di trattativa. In questa fase si cerca di delineare i parametri generali del / dei contratti e valutare i vincoli di budget e di tempistiche, le prestazioni da erogare e le tecnologie da utilizzare.
- **Completamento fase di analisi**: un'altra fase di negoziazione che potrebbe attivarsi è successiva alla conclusione del periodo di analisi da parte del fornitore sui requisiti e

⁷⁵ Farina M., (2018). I contratti informatici, Editore Key, pp.116-118

gli obiettivi del cliente. In questo senso, è molto probabile che si attivi una discussione in merito alle proposte individuate e all'offerta da sottoporre: proprio per questo motivo, è probabile che le due parti ricomincino a negoziare per trarre il maggior profitto ⁷⁶.

- **Durante la fase di implementazione:** non è raro durante i progetti di implementazione IT che, in fase di sviluppo, nascano nuove esigenze. Infatti, può accadere che ci siano nuovi requisiti che si manifestano in corso d'opera da parte del cliente e di conseguenza l'esigenza, eventualmente, di risorse o strumenti aggiuntivi necessario al raggiungimento dell'obiettivo finale. Pertanto, si attiverà una nuova fase di negoziazione supplementare tra cliente e fornitore per adeguare il contratto alle nuove esigenze emerse, per quanto concerne l'aggiornamento di costi, di tempi di consegna ed eventuali responsabilità sul funzionamento.
- **Contratto di assistenza e manutenzione:** anche in questo caso, è possibile che le due parti negozino i termini di un contratto di manutenzione del software o assistenza in un momento post go-live. Come si è già accennato, non è obbligatorio ma è molto comune che un cliente sottoscriva un contratto di supporto dell'applicativo IT.

2.1.2 Alta contrapposizione di obiettivi fra cliente e fornitore

Una caratteristica tipica del modello classico è quello della contrapposizione di obiettivi tra le due parti in essere, cliente e fornitore. Mentre, come si vedrà più avanti, nel modello cloud è spesso difficile negoziare i contratti in base agli scopi e ai requisiti del cliente, specialmente con i grandi player internazionali. In molti casi i contratti vengono “personalizzati” sulla base degli obiettivi dei servizi e del progetto.

Come si avrà modo di analizzare nelle pagine successive del lavoro di tesi, quando si parla di implementazione di un modello di architettura cloud, risulta sovente complessa la fase di negoziazione dei contratti in funzione degli scopi e dei requisiti specifici del cliente,

⁷⁶ Di Gabriele F., Italiano A., “I contratti di cloud computing: Comprendere, affrontare e negoziare i contratti”, Franco Angeli editore, 2017

particolarmente quando si ha a che fare con i grandi provider internazionali, i quali spesso tendono ad erogare servizi preconfigurati ⁷⁷ con pochi margini di negoziazione essendo poi tali contratti riconosciuti come “d’adesione”. In numerose circostanze, nel modello di implementazione inteso come classico, invece, i contratti vengono 'personalizzati' tenendo conto degli obiettivi dei servizi e delle esigenze specifiche del progetto.

In questo senso, se nel primo caso è più usuale che il cliente si adegui alla proposta del fornitore, nel secondo è comune che ci sia uno o più momenti di negoziazione e dialogo per incentrare il contratto (o i contratti) su quello che si vuole implementare.

È chiaro che, in fase di negoziazione, diventeranno ben palesi i diversi obiettivi degli attori coinvolti che, non è detto siano sempre in netta contrapposizione. Da un lato c’è il cliente che è spinto dalla realizzazione di un progetto funzionale ed efficiente, consegnato nelle tempistiche prefissate e con l’intenzione di spingere verso il basso il prezzo proposto dalla controparte; dall’altro c’è poi il fornitore i cui obiettivi sono prevalentemente rivolti all’ottimizzazione degli interventi da effettuare, delle figure da coinvolgere e alla massimizzazione dei profitti.

Nella contrapposizione tra gli obiettivi è possibile sottintendere anche la distinzione tra obbligazioni di mezzi e di risultati in relazione alle prestazioni fornite. In via generale è possibile stabilire che il cliente tenda a stabilire una negoziazione con l’interesse di raggiungere un’obbligazione di risultato: ciò significa che l’obiettivo del cliente / creditore è quello di raggiungere il risultato prefissato e quindi il contratto stesso sarà rispettato solo quando la prestazione o servizio in capo al debitore potrà dirsi completamente raggiunta in maniera efficiente.

Contrariamente, per il fornitore lo scopo è il raggiungimento di un’obbligazione di mezzi e non di risultato: il suo interesse, infatti, è quello di rispettare e garantire lo sviluppo o il supporto richiesto ma non garantire un risultato soddisfacente ⁷⁸.

2.1.3 Asimmetria informativa

Un elemento imprescindibile in qualsiasi relazione, specialmente se delineata dalla stipula di

⁷⁷Campagnoli MN., “Il cloud computing: vantaggi e problematicità”, pag 120

⁷⁸ <https://www.ht-avvocati.it/obbligazioni-debiti-crediti/debiti-crediti-tipi-obbligazione/obbligazione-mezzi-risultato.php>

uno o più contratti, è l'informazione. Prima di stipulare qualsiasi accordo, è necessario che entrambe le parti, con una maggiore attenzione per il cliente, abbiano tutte le informazioni, a livello trasversale, sui contenuti e le conseguenze di quello che stanno per firmare. Qualora questo non sia rispettato, l'asimmetria informativa diventa un rischio importante nella buona riuscita della relazione stessa può portare a fraintendimenti o a una valutazione errata delle attese e delle risorse indispensabili per la definizione del progetto.

Dunque, alla base dell'asimmetria informativa vi è sempre una delle parti che si porrà in una situazione di vantaggio rispetto all'altra proprio perché vi sarà una parte di informazioni che non sarà equamente condivisa e per la disparità di cultura informatica tra le parti ⁷⁹.

Uno dei territori in cui l'asimmetria informativa crea maggior differenza tra le parti è quella relativa ai costi delle prestazioni: è comune infatti che, oltre ai costi inseriti in fase negoziale, ce ne siano altri che sono in possesso al solo fornitore (si pensi ad esempio ai dati di mercato) che non vengono condivisi con il cliente. Spesso può capitare che tali situazioni si manifestino non solo in fase precontrattuale, e quindi durante il periodo di definizione degli accordi da prendere, ma anche in una fase successiva, e quindi dopo la stesura del contratto stesso: infatti, può capitare che durante la fase di implementazione le spese effettive possano superare quelle iniziali, creando un disallineamento tra le aspettative del cliente e la realtà ⁸⁰.

Ma ancora, rientrano nelle asimmetrie informative tutte quelle azioni o prestazioni non inserite in fase contrattuale: si pensi ad esempio, a requisiti non esplicitati o a richieste di modifiche di processi che vengono richieste in fase di sviluppo. Tutte queste informazioni non esplicitate rischiano di generare una situazione di malcontento che, a lungo andare, può minare la buona riuscita del progetto e compromettere la collaborazione tra le parti.

2.1.4 Rischio del non accordo

Uno dei principali rischi in cui si incorre nella formalizzazione di un contratto atto a soddisfare il requisito di implementazione di un gestionale è quello di non finalizzare appunto tutti quegli elementi necessari alla definizione del perimetro di intervento e delle componenti tecnologiche necessarie per un cliente ⁸¹. Tipicamente tale rischio risulta essere più alto per

⁷⁹ Iaselli M., (2019). *Lezioni di informativa giuridica*, Key Editore, p.222

⁸⁰ Gallo P., (2007), *Asimmetrie informative e doveri di informazione*, in "Rivista di diritto civile"

⁸¹ <https://www.riskmanagement360.it/analisti-ed-esperti/software-le-varie-tipologie-di-contratti/>

l'azienda cliente rispetto al fornitore.

Questo fenomeno nasce in quanto il fornitore, si prenda l'esempio tipico di una società di consulenza, lavora con diversi clienti al fine di massimizzare il proprio obiettivo, ovvero il ritorno economico e, quindi potrebbe non riuscire a sancire tutti i contratti proposti, mentre per l'azienda cliente il contratto è fondamentale per il raggiungimento dei suoi obiettivi aziendali, in quanto rappresenta il documento fondamentale dove tutti gli elementi vengono formalizzati. È anche vero che, al fine di ridurre il rischio di non accordarsi su determinati aspetti, le aziende fornitrici possono introdurre determinate figure atte proprio alla gestione commerciale del tutto, ovvero i Vendor Manager ⁸².

Oltre a questi aspetti, il fornitore ha la possibilità di scegliere i clienti con cui vuole lavorare, mentre il cliente potrebbe dover affrontare delle conseguenze non positive se non riesce a finalizzare il contratto entro un certo periodo di tempo. Questo fattore di rischio è estremamente più sensibile quando il cliente ha un bisogno urgente di implementare il software o il servizio fornito dal fornitore. In breve, il cliente ha un maggiore interesse a finalizzare il contratto rispetto al fornitore, e quindi il rischio di non finalizzare il contratto è solitamente più significativo per il cliente ⁸³.

Tipicamente, le situazioni d'emergenza sono indicative di un possibile non accordo che va ad innescare poi un processo oneroso di erosione dell'effort sia delle persone del team del fornitore che del cliente stesso. In questi casi, magari tali situazioni possono nascere in quanto non sono stati tenuti conto alcuni fattori all'interno della definizione del perimetro contrattuale ⁸⁴:

1. **Scarso coinvolgimento del top management:** spesso l'esigenza di implementare un software parte dalle aziende che hanno una funzione IT interna che, attraverso gare d'appalto o altri meccanismi, richiedono servizi predefiniti i quali però non rispecchiano in toto quelle che sono le reali esigenze del management.
2. **Cambiamento di uno / più processi di Business dell'azienda durante lo svolgimento del progetto:** è sovente che nel definire i processi e gli ambiti all'interno

⁸² <https://assets.kpmg.com/content/dam/kpmg/it/pdf/2018/02/Hybrid-IT-at-scale.pdf>

⁸³ Di Gabriele F., Italiano A., "I contratti di cloud computing: Comprendere, affrontare e negoziare i contratti", Franco Angeli editore, 2017, pag. 17

⁸⁴ H. Barki, S. Rivard, and J. Talbot, Toward an Assessment of Software Development Risk.

di un contratto, non si tengano conto di eventuali cambiamenti che sono in essere nell'azienda generando così dei gap tra l'AS-IS ed il TO-BE. In questi casi, non accordandosi specificatamente sulla situazione reale, spesso i fornitori sono chiamati a gestire le cosiddette *change request* che rappresentano per il cliente un ulteriore costo non previsto in sede di pianificazione.

3. **Assenza di individuazione delle responsabilità durante il ciclo di vita del progetto e del sistema:** tipicamente in un contratto di implementazione, è necessario definire una matrice RACI ⁸⁵ (Responsible, Accountable, Consulted, Informed) nel quale viene definita la gerarchia di ruoli e responsabilità nelle decisioni attinenti ad un progetto. Questo aspetto può rappresentare un elemento di non accordo in quanto la mancata individuazione di un soggetto responsabile può comportare la messa in atto di determinate decisioni che possono essere in linea o non con quanto desiderato dal cliente.

4. **Identificazione incompleta dei requisiti del sistema:** la mancata identificazione e definizione completa dei requisiti durante l'analisi impedisce una valutazione accurata delle risorse (economiche e umane), dei tempi e delle tecnologie necessarie per implementare il sistema. Questo aspetto può essere sia generatrice delle problematiche sopra esposte che una diretta conseguenza della stessa. La mancata valutazione di determinati elementi porta ad eventi di litigation tra cliente e fornitore che possono generare degli extracosti a danno del progetto e del budget preventivato per la gestione dello stesso.

Questi aspetti appena delineati, sono solo una sintesi di quelli che sono gli aspetti che possono innescare situazioni di non accordo. Queste fattispecie possono essere poi combinate con la possibilità di gestione di molteplici contratti, come analizzato nei paragrafi precedenti, e quindi generare un caos contrattuale che può indurre ambo le parti a non valutare o a sottovalutare determinate componenti necessarie alla buona riuscita del progetto. Pertanto, si può dire che il modello classico risente di aleatoria e, allo stesso tempo, discrezionalità delle

⁸⁵ <https://softwarebusiness.it/la-matrice-raci-nella-definizione-di-ruoli-e-responsabilita-nel-sistema-sap/>

parti in causa che può generare situazioni poco chiare.

2.1.5 Fattore tempo

Il cliente, di solito, subisce il maggior costo in caso di prolungamento dei tempi durante le negoziazioni ⁸⁶. Il tempo è cruciale per il cliente: se sta negoziando, ha un obiettivo da raggiungere e i ritardi possono causare problemi. Se non firma il contratto, non può realizzare il progetto e il suo business ne risente. Ad esempio, se sto trattando con un fornitore per un sistema informativo, il fornitore sa che alla fine dovrò decidere tra firmare il contratto o restare senza il sistema. Poiché non è presumibile continuare determinate attività senza il sistema informativo, il fornitore ha un vantaggio negoziale e sono costretto a firmare entro un certo tempo.

Sulla base di questa premessa, il fattore tempo assume due connotati precisi a secondo del momento contrattuale nel quale ci si trova.

- **Fase di start:** se la definizione del contratto di base richiede più tempo del previsto, è possibile che il cliente vada in sofferenza rispetto a determinate circostanze. Si pensi al caso della fatturazione elettronica. In quel caso il cliente necessita di software abilitati alla comunicazione con lo SDI e, di conseguenza, deve anche rispettare delle scadenze stabilite dalla legge per la trasmissione delle fatture. In questa circostanza, la lentezza del processo di formalizzazione può arrecare un maggior costo per il cliente, il quale non solo non riesce ad avere un software ma rischia anche di andare incontro a penali legate dal non rispetto della trasmissione delle fatture. Al fine di incorrere in tali circostanze, solitamente, negli accordi commerciali, il rapporto tra cliente e fornitore prevede anche deroghe a quanto previsto dalla legge, ovvero la possibilità di iniziare determinate attività nelle more della formalizzazione. Questo trattamento di maggior favore potrebbe giovare al cliente che ha esigenza di implementare determinate funzionalità ma, potrebbe essere nocivo per il fornitore che eroga risorse e tempo per un'attività senza aver modo di consuntivare i costi.

⁸⁶ Di Gabriele F., Italiano A, "I contratti di cloud computing: Comprendere, affrontare e negoziare i contratti", Franco Angeli editore, 2017, pag. 19;

- **Fase di implementazione:** al fine di avere un controllo su questi aspetti, è sovente prevedere degli accordi di performance basati su determinati KPI ⁸⁷ che consentono al cliente di monitorare se il progetto in essere è nelle tempistiche. Questi KPI devono essere ben stabiliti all'interno del contratto altrimenti si rischia di non aver un'interpretazione univoca di questi e, di conseguenza, delle ulteriori perdite di tempo a danno del cliente.

Il fattore tempo quindi, alla stregua del rischio di non accordo, rappresentano un ulteriore elemento critico nella gestione di contratti complessi previsti nel cosiddetto modello classico.

2.1.6 Implementazione di un nuovo sistema informativo con Business Analyst

In questo contesto di molteplici fattori, vi è una figura professionale che viene sempre più spesso adoperata da parte delle aziende clienti per analizzare processi di miglioramento dei vari processi aziendali. Prima di tutto, ha il compito di raccogliere e documentare il requisito di eventuali progetti da implementare: è una figura, quindi, che diventa protagonista sin dai primi momenti negoziali. Come diretta conseguenza, il Business Analyst dovrà progettare, sulla base delle informazioni raccolte, soluzioni efficaci tali da rispondere positivamente alle esigenze del cliente. Oltre a nuove implementazioni, uno dei suoi compiti è quello di analizzare processi già esistenti con il fine ultimo di valutare il corretto funzionamento ma anche di identificare aree da poter migliorare.

Come appare già evidente da queste prime informazioni, il Business Analyst è una figura cruciale nella comunicazione tra i vari settori di un'organizzazione in quanto, tra raccolta di requisiti e implementazione vera e propria, dovrà interagire con tutte le figure aziendali, quali stakeholders, utenti e team di sviluppo. Appare chiaro, allora, che l'analista business abbia tutte le competenze tecniche, di sviluppatore ancor meglio e anche competenze trasversali, quali comunicazione e problem solving, per metter tutti d'accordo e arrivare all'obiettivo ⁸⁸.

⁸⁷ <https://www.entersoftware.it/kpi-aziendali/>

⁸⁸ <https://www.egovaleo.it/geek-lab/business-analyst-cosa-fa-e-competenze/>

L'analista business può essere poi coinvolto in tutta la fase gestionale del progetto e quindi dalla fase di pianificazione, eventuali modifiche *in fieri*, sempre rientrando nei tempi di consegna e nel budget configurato, fino alla stesura di procedure di validazione di quanto progettato ⁸⁹.

Dal punto di vista contrattuale, la fase di individuazione dei requisiti di business parte dopo aver stipulato il contratto tra le controparti. Tale contratto infatti ha insita anche la parte di analisi dell'implementazione in essere e, per questo, si tratta di un contratto che verrà determinato in corso d'opera e, per questo, è determinabile. Tutti gli aspetti importanti, quali durata del contratto e costi, potranno essere concretamente definiti a fine analisi.

2.2 Prassi contrattuale per cloud computing

Come già anticipato nelle pagine precedenti, soluzioni di cloud computing si stanno diffondendo su larga scala, specialmente dovuto al grande utilizzo di internet da parte di industrie e settori. Nonostante il crescente impiego del cloud computing, che con il tempo si sta affermando come un punto di riferimento dell'*information technology*, ad oggi manca una consolidata normativa che disciplini l'assetto giuridico della contrattualistica del cloud computing e per tale ragione, non si può evitare di attenzionare tre problematiche legate alla prassi contrattuale.

2.2.1 Asimmetria negoziale

Quando si parla di asimmetria negoziale all'interno del contesto contrattuale, si fa riferimento ad una disparità, che in taluni casi è particolarmente marcata, del potere contrattuale tra le parti in essere. Come accennato, un contratto di cloud computing coinvolge e si basa prevalentemente sulla relazione tra due parti principali: da una parte un Fornitore che gestisce la piattaforma o i servizi software offerti e dall'altra il Cliente finale, il quale sceglie ed usufruisce dei servizi cloud forniti dal fornitore. Solitamente tale asimmetria negoziale, proprio in virtù di una non consolidata disciplina giuridica, è maggiormente sbilanciata in

⁸⁹ <https://vitolvecchia.altervista.org/professione-informatica-la-figura-del-business-analyst/>

favore del Fornitore ⁹⁰.

Appare evidente quindi che i contratti in materia di cloud computing non sono il risultato di un accordo tra le parti interessate quanto piuttosto un vincolo che inibisce le esigenze del cliente e che non considera la trattativa tra le parti: ciò è facilmente spiegato in quanto la conclusione degli accordi avviene solitamente tramite l'adesione a moduli on line.

Le ragioni possono essere molteplici e non di facile risoluzione.

Prima di tutto, uno dei principali elementi che conduce all'asimmetria negoziale riguarda la disparità di informazioni e conoscenze tra le parti: in molti casi, infatti, il fornitore è una multinazionale dei servizi cloud mentre il cliente può anche essere una piccola azienda che manca delle informazioni della controparte sia dal punto di vista quantitativo che qualitativo. C'è quindi una differenza nel potere di mercato dei due attori coinvolti, una delle quali dominante rispetto all'altra e questo conduce al fatto che il cliente finale spesso sottoscrive contratti di cui non ha piena conoscenza e che quindi non tutelano pienamente i suoi interessi ⁹¹. Il fornitore, quindi, ha una maggiore quantità di informazioni non solo sulle caratteristiche del servizio offerto, ma anche di eventuali costi nascosti e di politiche di sicurezza delle prestazioni garantite.

Questi aspetti sopra citati si collegano ad un'altra caratteristica intrinseca dei contratti di cloud computing, ovvero la standardizzazione del contratto stesso: si tratta, infatti, di contratti concepiti *ex ante* da parte del fornitore che quindi stabilisce previamente termini e clausole contrattuali che non lasciano margine di modifica, negoziazione da parte del cliente o rinegoziazione nel corso del tempo. La natura stessa di tali contratti li rendono estremamente vincolanti e rigidi, con scarsa o quasi nulla possibilità di modifica e personalizzazione.

Il divario tra le due parti contrattuali diventa ancora più grande in occasione delle clausole contrattuali, le quali sanciscono in maniera del tutto rilevante il dislivello di diritti e obblighi tra le parti. Si pensi, ad esempio, alle clausole relative alla deresponsabilizzazione verso eventuali danni e malfunzionamenti, verso la perdita di dati e accesso da parte di terzi ma anche clausole riguardanti la risoluzione dei rapporti. In questo contesto, infatti, l'asimmetria negoziale è particolarmente evidente in quanto, all'interno dei contratti di cloud computing, vengono inserite clausole che rendono difficile o impossibile la cessazione dei contratti, come

⁹⁰ Faggioli, G., & Italiano, A. (2017). *I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider*. Franco Angeli.

⁹¹ Iaselli M., (2019). *Lezioni di informatica giuridica*, Key Editore, p.221

l'impedimento all'utente finale di trasferire i propri dati ad un altro fornitore o la possibilità di farlo previo pagamento di costi ingenti ⁹².

2.2.2 Struttura contrattuale

Uno degli aspetti più controversi relativamente alla contrattualizzazione in materia cloud riguarda la natura e la struttura stessa dei contratti in essere.

Prima di tutto, va chiarito che un contratto di cloud computing non è specificamente e direttamente disciplinato all'interno del nostro ordinamento e pertanto viene considerato come un contratto di servizio atipico o contratto misto: si parla, infatti, di un modello che si basa non più sulla proprietà delle risorse informatiche e quindi sulla diretta gestione di queste da parte di un cliente, ma piuttosto sull'erogazione di un servizio che è possibile solo attraverso l'accessibilità a risorse messe a disposizione da un fornitore.

Per tale ragione, è anche piuttosto comune che un contratto di cloud computing venga adattato a partire da contratti inizialmente concepiti e previsti per le licenze software *on-premise* con l'inserimento di clausole, deroghe e nuove condizioni. Tutto questo fa in modo che il customer si imbatte in una complessa rete di documentazione contrattuale che, non è insolito, conduce all'esigenza di doversi servire di un supporto legale adeguato col fine ultimo di comprendere pienamente quello che si sta sottoscrivendo ⁹³.

Tendenzialmente, per quanto concerne la struttura di tali contratti, questi sono composti da quattro parti, alle quali si vanno ad aggiungere documentazione tecnica a corredo:

- 1) **Condizioni generali del contratto:** definiscono i *terms of service* che sono alla base del contratto e si riferiscono alle modalità attraverso le quali il servizio verrà offerto, con specifica attenzione alla durata del contratto, le condizioni di risoluzione, il compenso da versare ma anche le leggi applicabili;

- 2) **Livelli qualitativi / quantitativi dei servizi offerti:** a tal proposito, è fondamentale

⁹² S. Branshaw, C. Millard, I. Walden, *Standard contracts for cloud services*, in C. Millard (a cura di), *Cloud Computing Law*, Oxford 2014, pp. 44-46.

⁹³ Faggioli, G., & Italiano, A. (2017). *I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider*. Franco Angeli.

stabilire specifiche metriche che determinino la qualità del servizio offerto. Di fatti, la presenza degli SLA (Service Level Agreement) hanno proprio lo scopo di definire i livelli di performance garantiti dal provider e di verificare il rispetto e la conformità delle prestazioni. Tali parametri, possono riguardare sia la misurazione di performance quantitative che di solito riguardano la velocità del trasferimento dati e la capacità di archiviazione dati, il tempo di inattività e il servizio di supporto al cliente (ad esempio, durante le ore di lavoro del cliente o 24/7) ⁹⁴, ma anche tempi di risoluzioni di eventuali problemi o tempi di prima risposta, accessibilità alle piattaforme; ma delineano anche le conseguenze penali o crediti di servizio qualora il fornitore non riesca, per qualsivoglia motivo, rispettare e garantire quanto presente nel contratto stipulato ⁹⁵. I parametri di performance qualitativi, invece, possono riguardare l'eliminazione dei dati, la sicurezza e la protezione dei dati ma anche requisiti di localizzazione dei dati e portabilità ⁹⁶.

- 3) **Policy riguardante gli obblighi comportamentali di ambedue le parti:** è importante che sia il provider sia il customer si impegnino a rispettare quanto presente nel contratto firmato: le policy inserite servono proprio a stabilire quali sono le giuste regole di comportamento da rispettare per garantire un rapporto leale e corretto. Ad esempio, vengono inserite nelle policy comportamentali i canali di comunicazione ammessi e previste tra le due parti o le tempistiche di risposta attese, ma anche eventuali criteri per il monitoraggio delle attività o la creazione di report per valutare l'andamento del servizio. In quest'ottica possono rientrare anche gli *Acceptable Use Policy* (AUP), che sono volti a definire in quali contesti e in quali condizioni un fornitore è legittimato ad interrompere il servizio offerto successivamente ad un utilizzo improprio e non previsto dei software da parte dell'utente finale ⁹⁷.

⁹⁴ "Notes on the Main Issues of Cloud Computing Contracts," a cura dell'Uncitral- United Nations Commission on International Trade Law, 2019, cit., p. 14.

⁹⁵ Limone M., (2018). Cloud computing. Aspetti contrattuali, risvolti normativi e tutela della privacy, Youcanprint, pp.58-59

⁹⁶ "Notes on the Main Issues of Cloud Computing Contracts," a cura dell'Uncitral- United Nations Commission on International Trade Law, 2019, cit., p. 14.

⁹⁷ "Notes on the Main Issues of Cloud Computing Contracts," a cura dell'Uncitral- United Nations Commission on International Trade Law, 2019, cit., p.12

4) **Privacy e trattamento dei dati.** Quest'ultimo elemento è particolarmente importante e critico. È prerogativa dei contratti di cloud computing l'inserimento di un apparato che tenga conto della privacy, in virtù della grande quantità di dati sensibili e delle operazioni di trattamento, tra i quali configurano elaborazione e trasmissione di dati. Il trattamento dei dati è disciplinato dal Reg. 2016/679, anche conosciuto con l'acronimo GDPR (*General Data Protection Regulation*), che entra ufficialmente in vigore il 25 maggio del 2018.

Prima di tutto, un elemento fondamentale su cui il nuovo regolamento pone l'attenzione riguarda l'esigenza di tutelare equamente il diritto e la privacy dei dati personali dei cittadini europei, quindi indipendentemente dalle nazioni considerato l'enorme flusso di dati nella nuvola che chiaramente non conosce confini nazionali. Lo scopo di tale regolamento è quello di stabilire da un lato che il trattamento dei dati sia sempre lecito, corretto e trasparente nei confronti del cliente finale e che questi siano conservati in maniera adeguata a tutto il periodo in cui è attivo il contratto, mentre dall'altro che il consenso dato dall'interessato sia sempre libero, non-condizionato e basato su una piana e chiara informazione ⁹⁸.

Proprio per quanto sopra accennato, i contratti di cloud computing si presentano come particolarmente complessi proprio in virtù della molteplicità e diversificazione degli aspetti da dover trattare, in maniera più o meno completa.

2.2.3 Trasparenza

Un'altra problematica rilevante è caratterizzata dalla poca trasparenza di informazioni presenti nei contratti. Tale elemento di poca trasparenza, che va a collegarsi ai due precedentemente indicati, riguarda aspetti generali e specifici delle prestazioni fornite: si parla, ad esempio, di una deresponsabilizzazione da parte del provider, poche o anche nulle garanzie sulla qualità del servizio, che si collega poi all'impossibilità per il client di poter configurare in maniera personale il servizio proposto.

⁹⁸ Campagnoli M.N, (2018), Buone e/o cattive ragioni del cloud. Considerazioni alla luce del General Data Protection Regulation (GDPR), Rivista giuridica on-line, ISSiRFA, CNR, p.5-8

Le informazioni, solitamente, vengono fornite in maniera poco dettagliata e generica, e sono di difficile reperimento già in fase precontrattuale: questo primo aspetto mette il cliente sin dall'inizio in una fase di svantaggio rispetto alla controparte in quanto non permette di poter valutare attentamente le diverse offerte proposte dal mercato e scegliere con un quadro complessivo chiaro ⁹⁹. Ma tale criticità riguarda poi anche lo stesso testo del contratto che possono delinarsi come poco chiare e comprensibili da parte del cliente.

- Da un lato è comune che le clausole inserite siano scritte con terminologia tecnica e in taluni casi anche errata: spesso sono il risultato di una traduzione inesatta e di una terminologia non correttamente interpretata, magari perché derivanti dalla traduzione di contratti originariamente redatti in una lingua straniera.
- Dall'altro, invece, potrebbe anche accadere che in un contratto alcuni aspetti vengano solo accennati e quindi non trattati in maniera specifica, al punto di dover spingere il cliente a richiedere informazioni aggiuntive per chiarire eventuali ambiguità e dubbi

¹⁰⁰.

⁹⁹ Faggioli, G., & Italiano, A. (2017). *I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider*. Franco Angeli.

¹⁰⁰ Ibidem

Capitolo 3 – Contratti cloud: aspetti giuridici ed economici nella scelta di fornitura

3.1 Il contratto cloud: specificità ed aspetti normativi

Nei capitoli precedenti, si è avuto modo di delineare quelli che sono gli aspetti caratterizzanti del cloud computing, quale complesso sistema dei servizi web offerti da fornitori dedicati, definiti come *cloud provider (CSP)*. I vantaggi e gli svantaggi nella scelta di tale tecnologia sono diversi ma ciò che occorre delineare in questa sede è il profilo giuridico che guida la costituzione di un contratto di fornitura di un servizio cloud.

Il contratto di cloud è, come già accennato precedentemente nel lavoro, un contratto atipico¹⁰¹ e non identificabile nelle classiche forme tipizzate dal nostro Codice civile, a causa della peculiarità dell'obbligazione che sta alla base del servizio, la quale può assumere forme imprevedibili. Nonostante questa caratteristica, il contratto di cloud può essere comunque clusterizzato sulla base delle cinque caratteristiche imprescindibili¹⁰² dello stesso, ovvero:

1. i dati che non risiedono su server presenti concretamente, ma remoti;
2. la volatilità dell'archiviazione;
3. l'infrastruttura del fornitore;
4. il servizio attivabile online ed il ruolo preminente della connessione ad Internet;
5. il servizio offerto a consumo e il costo si basa sulla fruizione effettiva.

Queste caratteristiche sono fondamentali al fine di capire come un contratto del genere debba essere costituito e redatto al fine di tutelare i soggetti coinvolti in tutte le fattispecie necessarie all'erogazione efficace di un servizio.

Le clausole del contratto di servizi in cloud prevedono che l'utente possa porre fine al servizio

¹⁰¹ Faggioli, G., & Italiano, A. (2017). I contratti di cloud computing. Comprendere, affrontare e negoziare i contratti con i cloud provider. Franco Angeli.

¹⁰² <https://www.bucap.it/news/approfondimenti-tematici/continuta-operativa/cloud-caratteristiche.htm>

in qualsiasi momento e che il fornitore possa modificare unilateralmente il contratto, senza contraddittorio con l'utente, fatta salva la sua possibilità di recedere dal servizio. Inoltre, è consuetudine che il contratto sia redatto in lingua inglese, indipendentemente dalla provenienza dell'utente. Per contenere questa libertà del fornitore, mitigare la disparità di potere e proteggere gli utenti, si stanno introducendo nuove normative, tra cui il GDPR e le direttive settoriali.

Il *cloud*, infatti, rappresenta proprio un fatto contrattuale: mentre aumenta sempre più la richiesta di servizi cloud da parte delle imprese italiane ¹⁰³, i *provider* propongono condizioni generali di contratto e termini di utilizzi con modalità unilaterali, legato sempre alla questione che la convenienza di queste piattaforme sta nell'alta standardizzazione delle offerte e dei sistemi previsti.

Per questo motivo, il contratto tra aziende utenti e aziende fornitrici deve acquistare centralità ed ai fini di contrattazione di accordi più *fair*, pertanto, su questo tema subentra il codice di condotta sul *cloud computing* approvato dal *board* dei garanti dell'Unione Europea. Questo codice è stato approvato per i *Cloud Provider* ai sensi degli [artt. 40 e 41 del GDPR](#) ¹⁰⁴, su tutte le tipologie di servizi cloud (SaaS, PaaS, IaaS). Nonostante l'adesione al codice di condotta *Eu Cloud* per i fornitori non rappresenta una condizione di liceità per il trasferimento di dati personali verso un Paese Terzo, la sua adozione persegue l'obiettivo di aiutare gli utenti dei servizi *cloud* a identificare gli strumenti che danno maggiori garanzie di sicurezza e di promuovere la compliance in uno specifico settore.

Lo stesso vale per il codice di condotta del Cisce destinato ai servizi di infrastrutture cloud ¹⁰⁵.

Questi due codici sanciscono orientamenti pratici nel definire requisiti specifici, come prevede [l'articolo 28 del GDPR](#), per i responsabili del trattamento nell'UE ai quali si applicano, mentre, non si utilizzano in rapporto a trasferimenti internazionali di dati

¹⁰³ Il settore è valutato intorno ai 3,4 mld di euro nel 2020, con un balzo del 21% rispetto al 2019 - Dati Osservatorio Cloud Polimi (<https://www.altalex.com/documents/news/2021/11/23/contratto-cloud-raggi-x>).

¹⁰⁴ <https://www.altalex.com/documents/news/2021/11/23/contratto-cloud-raggi-x>

¹⁰⁵ Ibidem;

personali, poiché la loro adesione può essere utilizzata come elemento per dimostrare la conformità alle disposizioni di legge ¹⁰⁶.

Il contratto di servizi cloud, secondo quanto previsto dalle logiche *As a service*, si basa sulla fruizione di varie risorse informatiche, dettate secondo i bisogni degli utenti, *on demand*, secondo un modello *pay per use*. Nella fase della negoziazione, bisogna quindi attenzionare agli elementi essenziali quali: il prezzo, la performance, la sicurezza, l'interoperabilità, l'indipendenza e la compliance normativa. Altro elemento sensibile sono le clausole di esclusione della responsabilità, collegate a specifici fattori di rischio.

Lo schema di tali contratti è molto complesso e, come già accennato, non è disciplinato dal nostro ordinamento. Si tratta, infatti, di un contratto di servizio, come detto, atipico, che spesso presenta profili d'internazionalità ¹⁰⁷.

Da un primo excursus, appare evidente quindi quanto ci sia ancora da standardizzare rispetto alle tipologie di contratto. Ciò non toglie che però è possibile individuare le parti contrattuali, le quali normalmente sono tre ¹⁰⁸:

1. il *cloud provider* (CSP), noto anche come fornitore del servizio;
2. l'*amministratore di sistema*, responsabile della configurazione dei servizi offerti dal *cloud provider* e che svolge una funzione di interfaccia tra quest'ultimo e il cliente finale;
3. il *cliente finale* (*cloud consumer*), utilizzatore dello spazio di archiviazione e del servizio.

Le condizioni del contratto in esame comprendono:

¹⁰⁶ https://www.edpb.europa.eu/news/news/2021/edpb-adopts-opinions-first-transnational-codes-conduct-statement-data-governance-act_it

¹⁰⁷ <https://en.iusintech.com/il-contratto-di-cloud-computing/>

¹⁰⁸ <https://en.iusintech.com/il-contratto-di-cloud-computing/>

- le condizioni generali del servizio, che dettano la durata, il corrispettivo, la responsabilità, la risoluzione del contratto, la modalità di recesso ecc.;
- i livelli qualitativi del servizio offerto (o Service Level Agreement – SLA), che indicano i parametri del servizio offerto; le obbligazioni delle parti contrattuali (es. condizioni da rispettare affinché non si verifichi l’interruzione o la sospensione del servizio);
- le modalità di trattamento dei dati personali (Privacy Policy).

Una parte della dottrina ¹⁰⁹ ritiene che il contratto di *cloud computing* abbia natura di appalto di servizi (art. 1655 c.c.), poiché il risultato conseguito è affine a quello ottenuto attraverso i *contratti di outsourcing*. Un’altra parte della dottrina ¹¹⁰ ritiene che si tratti di un contratto misto, con elementi che si rifanno come citato all’appalto di servizi e altri riconducibili al contratto di licenza.

Nel contesto del cloud computing, i provider e i clienti amministratori, date le loro posizioni dominanti, spesso ricorrono a contratti per adesione, costituiti da clausole predisposte unilateralmente da uno solo dei contraenti ¹¹¹. In questo modo l’utente non riesce a determinare i contenuti e i livelli di sicurezza del servizio che acquista, tuttavia, nonostante le clausole siano predisposte unilateralmente, ha la possibilità di scegliere tra diversi fornitori di servizi cloud. Occorre però sempre tener presente che il contratto deve in primis essere redatto in forma chiara e trasparente. Infatti, la mancata trasparenza o chiarezza del contratto non consente una scelta appropriata ¹¹².

In definitiva, se occorre in questa sede delineare quelli che sono gli aspetti più importanti, è possibile considerare il seguente elenco ¹¹³:

¹⁰⁹ E. PRANDELLI, G. VERONA, “Vantaggio competitivo in rete, dal web 2.0 al cloud computing”, 2011.

¹¹⁰ F. PIROZZI, “Il cloud computing”, Giuffrè, 2016.

¹¹¹ <https://en.iusintech.com/il-contratto-di-cloud-computing/>

¹¹² R. MOSHER, Cloud Computing Risks, Usa, ISSA Journal, 2011.

¹¹³ <https://en.iusintech.com/il-contratto-di-cloud-computing/>

1. **La Responsabilità del Fornitore (CISP):** i contratti contengono clausole che escludono la responsabilità del provider per determinati danni e stabiliscono un limite di risarcibilità predeterminato.
2. **Il Service Level Agreement (SLA):** con cui il provider tratta i criteri di erogazione del servizio e i criteri di monitoraggio della qualità, in termini di legalità e sicurezza;
3. **La Protezione dei dati:** il contratto dovrebbe indicare le misure tecniche per tutelare i dati e i controlli di sicurezza.
4. **Il Disaster Recovery:** il contratto deve contenere l'indicazione del sito secondario da cui verrà erogato il servizio in caso di disastro, i tempi di ripristino dei servizi e i tempi di sincronizzazione dei dati tra i due siti.
5. **La Localizzazione dei data center e filiere di fornitura:** deve indicare in modo chiaro e trasparente i luoghi in cui i dati verranno trattati o conservati, anche nel caso in cui l'intermediario da cui si acquista il servizio si avvalga di subfornitori extra UE.
6. **I Soggetti responsabili della tutela dei dati personali (Privacy policy):** vanno regolamentati nel contratto gli obblighi e le reciproche responsabilità in relazione al trattamento dei dati e i doveri di assistenza e collaborazione che i responsabili e sub-responsabili devono garantire al titolare, ai sensi dell'art. 28 del GDPR.
7. **Le Modalità di Audit:** l'utente deve poter controllare il Cloud Service Provider per accertarsi che l'esercizio del servizio sia basato su norme valide ed anche per verificare l'effettiva protezione dei dati.
8. **Le Risoluzioni contrattuali (way-out):** l'utente dovrebbe poter far cessare gli effetti del contratto con determinate clausole risolutive espresse, se il servizio non è idoneo

114 115 116

Il regolamento europeo CE n. 593/2008, noto come "Regolamento Roma I" e sancito al posto della Convenzione di Roma del 19 giugno 1980 e della Convenzione di Bruxelles, prevede

¹¹⁴ G. COLANGELO, L'enforcement del diritto d'autore nei Servizi Cloud, in *Dir. aut.*, 2012, II, 174; A. MANTELELO, Il contratto per l'erogazione alle imprese di servizi di cloud computing, in *Contr. impr.*, 2012, IV-V, 1216.

¹¹⁵ A. MANTELELO, Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali, in *Dir. informaz. informat.*, 2010, 673

¹¹⁶ G. TROIANO, Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale: alla ricerca di un equilibrio tra diritti dell'utente e doveri del fornitore, in *Cyberspazio e diritto*, 2011.

l'applicabilità della legge dello Stato in cui risiede il consumatore al contratto ¹¹⁷. Il legislatore italiano non sancisce che il consumatore possa essere privato della tutela richiesta dal Codice del consumo, tuttavia, se l'utente è un'azienda, la tutela del consumatore non si applica e le clausole che limitano la responsabilità del cloud provider sono valide ¹¹⁸. Apparirà quindi importante affidarsi alla consulenza di esperti tecnici e giuristi, capaci anche di intervenire in caso di violazione dei diritti alla privacy o di violazione della cyber security.

3.1.1 La responsabilità del cloud provider

Un provider di servizi cloud, o CSP (Cloud Service Provider), è un'azienda di terze parti che fornisce risorse di computing scalabili a cui le aziende possono accedere on demand su una rete, tra cui computing, archiviazione, piattaforma e applicazioni basati su cloud. Rispetto a questo elenco di attività facenti parti di un servizio complesso da erogare da parte del fornitore, assume un ruolo rilevante la sicurezza informatica.

La sicurezza informatica si occupa dell'analisi del rischio, delle minacce, della debolezza e della protezione di un sistema informatico e dei dati in esso contenuti o scambiati tra gli utenti ¹¹⁹. I termini *information security* e *computer security* hanno in comune il fine ultimo di mantenere alcune proprietà dell'informazione, quali *confidentiality*, *integrity* e *availability* ¹²⁰.

La *confidentiality* consiste nel prevenire la rivelazione delle informazioni ad utenti o sistemi non autorizzati, impegnando il fornitore a garantire la privacy delle persone che sono in possesso di informazioni rilevanti.

Per quanto riguarda la *integrity* rappresenta la possibilità che i dati non possono essere

¹¹⁷ <https://en.iusintech.com/il-contratto-di-cloud-computing/>

¹¹⁸ *Convenzione 80/934/CEE sulla legge applicabile alle obbligazioni contrattuali aperta alla firma a Roma il 19 giugno 1980.*

¹¹⁹ PERRI, "Il cloud computing nelle imprese e nella pubblica amministrazione", Giuffrè, 2019.

¹²⁰ M. LIMONE, "Cloud computing. Aspetti contrattuali, risvolti normativi e tutela della privacy", 2015.

modificati senza che questo sia venga reso palese ^{121 122 123 124}.

La *availability* mira a rendere i dati disponibili in qualunque momento sia necessaria.

Questi sono i fondamenti base del trattamento delle informazioni che, nel contesto di responsabilità di un CSP, risulta fondamentale dichiarare nel contratto e monitorare costantemente durante l'erogazione del servizio. È così importante che, dal punto di vista organizzativo, si progettano ruoli e si assegnano responsabilità precise per ogni utilizzatore del sistema. Dal punto di vista tecnologico, vengono utilizzati diversi sistemi di protezione adatti al contesto che si vuole proteggere. È essenziale definire tempestivamente dubbi e problematiche, e per far questo si effettua un'analisi di rischio. Molto spesso, anzi quasi sempre, nelle implementazioni di piattaforme applicative come quella in cloud, è previsto che l'utente abbia una profilazione ad hoc, costruita dal CSP, con il quale si può controllare il cono informativo al quale una determinata persona può avere accesso.

Questo della gestione delle informazioni, è solo uno dei rischi ai quali bisogna far fronte. Il National Institute of Standards and Technology (NIST) definisce i rischi come “*a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization*” ¹²⁵. Da questa affermazione, emerge quindi il vincolo di vulnerabilità derivante dalla gestione di un contratto di tale genere.

Un provider di servizi cloud spesso si identifica come una società IT che offre risorse di *computing* scalabili *on demand* come potenza di *computing*, archiviazione di dati o applicazioni su internet.

Ci sono svariati fattori da verificare nella valutazione dei provider di servizi cloud.

¹²¹ A. OSNAGHI, *Pubblica amministrazione che si trasforma: «Cloud Computing», federalismo, interoperabilità, Amministrare*, 2013, I, 59.

¹²² D. GLORIO, *Il Cloud Computing nella P.A. e nei servizi demografici*, *Lo Stato civile italiano*, 2013, III, 37

¹²³ G. Queiroli, *Is Apple clouding US (and other countries') taxes?* in *Dir. Pratica tributaria internaz.*, 2013, II, 459

¹²⁴ M. ROTENBERG, *Un dialogo su diritti e libertà civili nell'era tecnologica: social networking, Facebook, body scanning, cloud computing, geotagging e behavioral privacy*, 2010.

¹²⁵ JABBOR, K., & POISSON, J. "Cyber Risk Assessment in Distributed Information Systems." *The Cyber Defense Review*, Vol. 1, No. 1 (Spring 2016), pp. 91-112 (22 pages).

In primis il **costo**, uno dei fattori principali per prendere una decisione ^{126 127}. È utile valutare sia i costi diretti dell'utilizzo del servizio sia eventuali costi indiretti, come l'assunzione di talenti o il ritiro di sistemi *on-premise*.

Poi vi è la **funzionalità e processi digitali**. Oltre ad esaminare i prodotti e servizi cloud disponibili, è fondamentale verificare la capacità di un CSP di soddisfare le tue esigenze IT attuali e future dell'azienda. È utile valutare la facilità con cui è possibile gestire ed eseguire il *deployment* dei servizi, così come l'integrazione disponibile per le applicazioni *business critical*.

Deve essere inoltre **attendibile**. La fiducia nel proprio provider di servizi cloud è un prerequisito per una relazione di successo. È importante fare una valutazione preliminare onesta di ciò che serve veramente da un CSP e capire se è in grado di soddisfarle.

Un altro aspetto da considerare l'**ecosistema aperto**. Sempre più spesso, le soluzioni proprietarie non soddisfano i requisiti tecnici delle aziende moderne. È quindi cruciale valutare quanto sia aperto un *provider* di servizi cloud. Un provider di servizi cloud di alto livello dovrebbe sfruttare tecnologie *open source* e soluzioni interoperabili che garantiscano coerenza e gestione efficace in qualsiasi contesto ¹²⁸.

Infine, per quanto riguarda la sicurezza, il CSP fornitore deve dimostrare di poter **proteggere i dati dell'azienda e dei clienti** ¹²⁹. Questo include la valutazione di qualsiasi aspetto, dall'infrastruttura ai criteri di sicurezza, dalla gestione delle identità al *backup* e alla conservazione dei dati. È essenziale conoscere quali sono i controlli disponibili per garantire la sicurezza fisica del data center, come le misure di salvaguardia dell'ambiente, il ripristino di emergenza e i piani di continuità aziendale documentati ¹³⁰.

¹²⁶Mantelero, *Il contratto per l'erogazione alle imprese di servizi di cloud computing*, in *Contr. e Impr.*, 4-5, 2012, p. 1217 ss.

¹²⁷Faggioli, Italiano, *I contratti di cloud computing*, Milano, 2017, p. 17.

Entrambi riprendono il fondamentale contributo di Rifkin ne "L'era dell'accesso", opera risalente al 2000.

¹²⁸L.M. VAQUERO, L. RODERO-MERINO, J. CACERES, M. LINDNER, "A Break in the Clouds: Towards a Cloud Definition," Vol. 39, N. 1, January 2009.

¹²⁹E. BELISARIO, "Cloud Computing", *Informatica Giuridica* – collana diretta da Michele Iaselli - eBook n.17, Altalex 2011.

¹³⁰E. BELISARIO, "Cloud Computing", *Informatica Giuridica* – collana diretta da Michele Iaselli - eBook n.17, Altalex 2011.

3.1.2 Limitazioni ed esclusioni della Responsabilità del Cloud provider

Molto spesso la necessità dei *cloud service providers* di gestire in modo coerente ed uniforme i vari rapporti contrattuali porta ad un'imposizione unilaterale di accordi rigidi, avverso i quali gli utenti finali non sono in grado di esplicare un effettivo potere negoziale^{131 132}. Bisogna quindi prestare attenzione non solo alle caratteristiche tecniche e alle condizioni economiche, ma anche ai termini contrattuali relativi all'utilizzo delle tecnologie cloud. Ciò vale sia che il *cloud consumer* abbia la forza contrattuale sufficiente per negoziare le condizioni del servizio, sia che debba subire un contratto standard, unilateralmente predisposto dal fornitore. Conoscere le criticità più diffuse nella contrattualistica dominante in quest'ambito può essere utile per indirizzare le scelte d'impresa¹³³, in funzione delle effettive esigenze aziendali, privilegiando determinati modelli di servizio o determinati fornitori piuttosto che altri¹³⁴.

Tra le clausole presenti negli accordi proposti al mercato dalla maggior parte dei provider ci sono le garanzie offerte dal provider¹³⁵. Queste garanzie stabiliscono che il servizio viene erogato "as is" o nelle condizioni in cui si trova, senza includere garanzie come quella di buon funzionamento, di conformità ad uno scopo specifico e di non violazione di diritti dei terzi. Nonostante molti accordi prevedano specifici SLA, in base ai quali il provider si impegna a garantire determinate soglie di disponibilità del servizio, nella maggior parte dei casi le clausole in materia di garanzie escludono che l'operatività del servizio stesso sia ininterrotta o priva di errori o che gli errori siano tempestivamente corretti.

Vi è poi la limitazione o esclusione di responsabilità: in modo uniforme, gli accordi aventi ad oggetto i servizi *cloud* prevedono una disciplina dettagliata per l'esclusione/limitazione

¹³¹ <https://www.zerounoweb.it/cloud-computing/contratti-cloud-le-clausole-da-tenere-d-occhio/#:~:text=In>

¹³² FAGGIOLI, Italiano, I contratti di cloud computing, Milano, 2017, p. 17. Entrambi riprendono il fondamentale contributo di Rifkin ne "L'era dell'accesso", opera risalente al 2000.

¹³³ FAGGIOLI G., ITALIANO A., "Contratti cloud, le clausole da tenere d'occhio" <https://www.zerounoweb.it/cloud-computing/contratti-cloud-le-clausole-da-tenere-d-occhio/>

¹³⁴ MANTELERO A., Il contratto per l'erogazione all'impresa dei servizi di cloud computing, in Contratto e Impresa, 2012.

¹³⁵ <https://www.zerounoweb.it/cloud-computing/contratti-cloud-le-clausole-da-tenere-d-occhio/#:~:text=In>

della responsabilità del *cloud provider* per ogni tipo di danno derivanti tanto dall'utilizzo come dall'impossibilità di utilizzo dei servizi oggetto di contratto, salvi i limiti inderogabili di legge ¹³⁶. Tra queste previsioni, vi sono le clausole di esclusione di responsabilità di quest'ultimo in ordine ai danni conseguenti ad eventi la cui previsione e gestione dovrebbe rientrare tra gli ordinari obblighi contrattuali del cloud provider: l'esempio più eclatante è la frequente clausola di deresponsabilizzazione per il caso della perdita dei dati del cliente.

C'è poi il diritto di modifica unilaterale delle condizioni contrattuali, che si riferisce alle clausole che concedono al provider il potere di modificare unilateralmente, a sua esclusiva discrezione, tutte le condizioni del servizio, azionabile sempre e in ogni momento del rapporto contrattuale, salvo il diritto di recesso accordato all'utente ¹³⁷. Un minimo livello minimo di tutela richiederebbe che se ci fosse bisogno di modifiche, queste non dovrebbero operare in senso peggiorativo per l'utente, che vengano portate a conoscenza dell'utente con modalità di comunicazione diretta e che diventino effettive solo al momento del rinnovo contrattuale ¹³⁸.

C'è poi la questione della sospensione o interruzione del servizio: si tratta di clausole che concedono al cloud provider la possibilità di sospendere il servizio in varie modalità, e possono minare l'equilibrio contrattuale in quanto spesso troppo generiche o indeterminate. Queste previsioni devono essere esaminate attentamente durante la fase contrattuale con il fornitore, considerando la natura specifica del servizio scelto, la sua rilevanza e importanza strategica per i processi aziendali. Una maggiore attenzione ai profili contrattuali può, infatti, orientare la scelta del servizio più conforme alle proprie esigenze e ridurre i rischi di danni derivanti da un inadempimento del fornitore ^{139 140}.

¹³⁶ M.G. LOSANO, Informatica Giuridica, in Dig. Civ., IX, Torino, 1993.

¹³⁷ A. MANTELERO, "Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali" Saggi, in Dir. dell'informazione e dell'informatica, 2010.

¹³⁸ <https://www.zerounoweb.it/cloud-computing/contratti-cloud-le-clausole-da-tenere-d-occhio/#:~:text=In>

¹³⁹ <https://www.zerounoweb.it/cloud-computing/contratti-cloud-le-clausole-da-tenere-d-occhio/#:~:text=In>

¹⁴⁰ ENISA, Cloud Computing Security Risk Assessment, 2009.

3.2 Patologie nella gestione dei contratti cloud: ripercussioni legali ed economiche

Al fine di analizzare quelle che possono essere ritenute ripercussioni legali ed economiche legate alle patologie dei contratti cloud, è necessario capire dapprima nella legge cosa è previsto e cosa può essere sancito al fine di ridurre al minimo il danno.

La volatilità di determinate situazioni dipende da quello che attualmente l'industria sta attraversando e il cloud, considerato un processo ad alto rendimento ¹⁴¹ ¹⁴², si interseca perfettamente con due importanti processi in corso: da un lato vi è la *servitization* ¹⁴³, dall'altra la transizione digitale.

La *servitization* può essere definita come lo slittamento nei modelli di business, caratterizzato dall'abbandono della logica centrata sul prodotto a favore di un'offerta più complessa composta e articolata. Secondo l'impostazione tradizionale di Vandermerwe e Rada, questa nuova strategia si compone di beni, servizi, support, self-service e conoscenza, ponendo al centro il servizio, in quanto personalizzato sulle esigenze del singolo cliente. Si è già detto del nesso fra cloud e mondo As-a-service e sul punto la comunicazione tace, mentre si nota che nell'era digitale *«la politica industriale deve integrare le nuove opportunità tecnologiche come ad esempio il cloud computing, i mega-dati e gli sviluppi della catena di valore dei dati, le loro applicazioni industriali in internet, le fabbriche intelligenti, la robotica, la stampa e il design 3-D»* ¹⁴⁴.

¹⁴¹ Guido Noto La Diega, "Il cloud computing. Alla ricerca del diritto perduto nel Web 3.0", estratto da "Europa e diritto privato, fasc. 2 – 2014,

https://www.researchgate.net/publication/269110088_G_NOTO_LA_DIEGA_Il_cloud_computing_Alla_ricerca_del_diritto_perduto_nel_web_30_Cloud_computing_In_Search_of_Lost_Law_in_the_Web_30_in_Europa_e_diritto_privato_2014_II_577-659

¹⁴² Là dove si legge che «il software di infrastruttura e il software di connettività per l'internet industriale costituiscono un ambito prioritario alla luce della loro crescente importanza e dovrebbero contribuire ad integrare processi ad alto rendimento, compreso il cloud computing».

¹⁴³ European Competitiveness Report 2011, Commission Staff Working Paper, 14-10-2011, SEC (2011) 1188 final, di accompagnamento alla com. 14-10-2011, Politica industriale: rafforzare la competitività, COM (2011) 642 final e, in dottrina, E. Rullani et al., Innovazione e produttività. Alla ricerca di nuovi modelli di business per le imprese di servizi (Milano 2012), spec. 197; D. Lalli-R. Lanzara, La *servitization* dei prodotti, Nuovi modelli di business e creazione di valore: la Scienza dei Servizi, a cura di L. Cinquini, A. Di Minin e R. Varaldo, Milano 2011.

¹⁴⁴ Consiglio dell'Unione Europea. "Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni: Per una rinascita industriale europea." Bruxelles, 23 gennaio 2014,

[https://www.senato.it/web/docuorc2004.nsf/6cc8889e3afb022fc12576ab0045bc47/17fa3a7a3ab5f149c1257c6d003dc95e/\\$FILE/05489_14_IT.pdf](https://www.senato.it/web/docuorc2004.nsf/6cc8889e3afb022fc12576ab0045bc47/17fa3a7a3ab5f149c1257c6d003dc95e/$FILE/05489_14_IT.pdf)

Sul tema dei rischi legati a questi aspetti, è interessante inserire nel discorso il tema discusso dall'«articolo 29»¹⁴⁵, elemento fondamentale nella costituzione di un assetto normativo atto a tutelare la fattispecie, in quanto tale articolo è volto a regolarizzare le tematiche sulla prevenzione dei danni legati all'adozione del cloud e dei servizi annessi. Tale articolo infatti analizza l'applicazione delle norme vigenti in materia di protezione dei dati enunciate nella direttiva 95/46/CE ai fornitori di servizi di cloud computing operanti nello Spazio economico europeo (SEE) e ai loro clienti.

In particolare, tale articolo, nel suo Parere n. 5 del 2012, traccia le possibilità di rischio quali^{146 147}:

- Mancanza di disponibilità dovuta alla scarsa interoperabilità
- Mancanza di integrità dovuta alla condivisione di risorse
- Scarsa possibilità di intervento, soprattutto per più fornitori
- Mancanza di isolamento

Questi aspetti non vanno sottovalutati, in quanto il contesto economico nel quale si muovono le aziende è mutevole in maniera costante e, pertanto, un possibile contratto cloud già attivo con un fornitore possa rappresentare un punto di forza o di debolezza per un'azienda cliente. Pertanto, è necessario tenere a mente gli aspetti evidenziati nella gestione di un contratto cloud.

Ciò che si evince dalla legge, sempre nel caso dei contratti atipici, è che si ricorre sempre alla stessa disciplina prevista dal Codice civile: così come avviene per i contratti di esternalizzazione, l'*outsourcing* si considera come base di partenza la disciplina dell'appalto (art. 1655 e segg, Cod. Civ.), ossia dell'appalto di servizi¹⁴⁸.

Per appalto si intende un contratto che prevede che il fornitore, definito come prestatore di servizi, poggia tali servizi su due elementi fondamentali: l'organizzazione dei mezzi necessari e la gestione degli stessi a proprio rischio.

Nello specifico del contratto di *cloud computing*, vi è inoltre l'obbligo di risultato che

¹⁴⁵<https://www.agendadigitale.eu/sicurezza/contratto-cloud-computing-la-guida-completa-ecco-come-funziona/>

¹⁴⁶ L. Sartori, Il Divario digitale. Internet e le nuove disuguaglianze sociali, Il Mulino, 2006.

¹⁴⁷ <https://www.agendadigitale.eu/sicurezza/contratto-cloud-computing-la-guida-completa-ecco-come-funziona/>

¹⁴⁸ <https://www.agendadigitale.eu/sicurezza/contratto-cloud-computing-la-guida-completa-ecco-come-funziona/>

vincola il fornitore a concludere quanto sancito in termini di incarico nei confronti del cliente. Infatti, nello stesso articolo del Codice civile, si stabilisce che nell'obbligazione di risultato il prestatore di servizi si libera dalle sue obbligazioni solo con il conseguimento del risultato stesso.

Considerando invece quella che è la causa ¹⁴⁹ ¹⁵⁰ del contratto, si può considerare il *cloud computing* come un contratto atipico dove il nucleo della disciplina è fornito dal contratto di somministrazione (Art. 1677 Cod. Civ.).

Pertanto, alla luce delle due discipline appena richiamate, è necessario sottolineare quelli che sono i requisiti essenziali da considerare per formalizzare un contratto di *cloud computing*, ovvero: la definizione dell'oggetto della prestazione, della valutazione dell'adempimento, le dichiarazioni e rappresentazioni, i diritti di controllo, accesso e verifica, garanzie e penali, responsabilità, protezione dei dati personali, sicurezza e tutele legali. Bisogna concretizzare un contratto di esternalizzazione su misura.

Dal momento che è un contratto atipico che si basa sulla disciplina del contratto di somministrazione, il contratto di *cloud computing* risulta come un'obbligazione di risultato per il fornitore di servizi; quindi, è essenziale individuare l'oggetto del contratto in termini di descrizione delle prestazioni dovute. Si afferma che sarebbe meglio ricorrere ad una combinazione di approcci per definire chiaramente il servizio offerto. Questo include una descrizione oggettiva del servizio prestato, mediante anche ricorso di appositi allegati o capitolati integrativi al contratto, insieme all'utilizzo di una delle formulazioni tracciate.

Per poter correttamente individuare la misura dell'esatto adempimento, è cruciale stabilire i vari requisiti chiave, oggettivi e misurabili, che definiscono chiaramente ciò che costituisce un adempimento completo per ciascuna delle prestazioni dall'oggetto del contratto. È altrettanto importante stabilire il livello di obiettivo obbligatorio da raggiungere per ogni parametro ¹⁵¹.

Una tecnica comune per ottenere questo risultato è la definizione e adozione di metriche concordate di misurazione che si fondano sulla definizione dei KPI, ovvero parametri

¹⁴⁹ Altalex: La causa è la funzione economico sociale del contratto o, come preferiscono altri, la funzione economico individuale (<https://www.altalex.com/documents/altalexpedia/2016/02/29/causa>).

¹⁵⁰ <https://www.agendadigitale.eu/sicurezza/contratto-cloud-computing-la-guida-completa-ecco-come-funziona/>

¹⁵¹ BERTONI A., Cloud Computing e trasferimento dati le questioni giurisdizionali (DRAFT), 2012.

oggettivi e misurabili associati alle prestazioni (permettono di scomporre l'oggetto del contratto in prestazioni specifiche che possono essere valutate in modo obiettivo), e sulla definizione dei SLA, ossia l'individuazione della misura che esprime il livello obiettivo da raggiungere, il quale è garantito dal prestatore dei servizi nell'adempimento degli obblighi contrattuali ¹⁵².

Bisogna poi predisporre delle protezioni contrattuali in caso di inadempimento, che possono essere rappresentate da cauzioni o garanzie fidejussorie, anche sotto forma di polizza fidejussoria o bancaria. Inoltre, è essenziale includere adeguate clausole penali per il caso di mancato rispetto dei SLA definiti contrattualmente ¹⁵³.

Inoltre, contrattualmente è fondamentale rispettare tali obblighi ¹⁵⁴:

- mantenere una giusta copertura assicurativa per tutta la durata del contratto, presso una compagnia assicurativa di adeguato *rating*;
- mantenere attive le certificazioni e aderire a codici di condotta di settore che siano state considerate nel processo di selezione del prestatore di servizi e stipula del contratto di affidamento del servizio di *cloud computing*.

Inoltre, va considerato che, se il contratto è disciplinato da *common law*, il regime giuridico sarà diverso rispetto dal nostro. In particolare, vi sarà una diversa impostazione nella definizione della colpa per inadempimento contrattuale e della colpa grave.

Tutti questi elementi elencati servono a mettere in luce i criteri di criticità che possono emergere durante l'utilizzo di un contratto di questo tipo e, di conseguenza, essere gestiti. Ne consegue che la mancata previsione di uno di questi elementi potrebbe comportare conseguenze legali ed economiche per l'azienda cliente.

Si pensi, ad esempio, a un contratto che non preveda la gestione degli SLA. Questi meccanismi di controllo sono utili affinché il funzionamento del sistema cloud venga mantenuto costantemente in determinati intervalli temporali, sulla base di ciò che l'operatore deve fare. Senza l'inclusione degli SLA nel contratto, il fornitore potrebbe non

¹⁵² <https://www.agendadigitale.eu/sicurezza/contratto-cloud-computing-la-guida-completa-ecco-come-funziona/>

¹⁵³ SICA S., ZENO- ZENOVICH V., Manuale del diritto dell'informazione e della comunicazione, 2006.

¹⁵⁴ <https://www.agendadigitale.eu/sicurezza/contratto-cloud-computing-la-guida-completa-ecco-come-funziona/>

sentirsi obbligato a rispettare le tempistiche previste, poiché la mancanza di specifiche indicazioni contrattuali potrebbe consentirgli una maggiore flessibilità nell'interpretazione delle situazioni e dei tempi di risposta. Ad esempio, qualora non siano previsti SLA ed un utente ha difficoltà ad inserire una fattura a sistema, il fatto che il fornitore si senta libero di non rispettare le tempistiche predefinite potrebbe comportare da parte sua una mala valutazione della situazione che, in virtù della sua rilevanza, potrebbe causare dei danni economici all'azienda. Pertanto, la stipula di capitolati e documenti aggiuntivi al contratto può essere considerata una forma di garanzia a favore del cliente.

3.3 Strategie di way out: diritto di risoluzione e recesso del contratto

Nonostante i numerosi vantaggi offerti dal cloud computing, è essenziale comprendere le strategie di "way out" disponibili agli utenti nel caso in cui si renda necessario terminare o modificare un contratto con un fornitore di servizi cloud.

La risoluzione giudiziale è definita nell'articolo 1453 del Codice civile che sancisce la risolubilità del contratto per inadempimento e prevede che nei contratti con prestazioni corrispettive, quando uno dei contraenti non adempie le sue obbligazioni, l'altro può a sua scelta chiedere l'adempimento o la risoluzione del contratto, salvo, in ogni caso, il risarcimento del danno. Tale richiesta può essere avanzata anche durante una causa già avviata per ottenere l'adempimento, ma una volta richiesta la risoluzione, non sarà più possibile richiedere l'adempimento. Dalla data della richiesta di risoluzione, l'inadempiente non potrà più adempiere all'obbligazione.

La risoluzione di diritto è stabilita all'articolo 1454, dove viene sancita la diffida a adempiere, si prevede che. Alla parte inadempiente l'altra può intimare per iscritto di adempiere in un congruo termine, con dichiarazione che, decorso inutilmente detto termine, il contratto si intenderà risolto. Tale risoluzione avviene mediante la diffida a adempiere. Questa procedura prevede che la parte inadempiente sia notificata per iscritto e le sia concesso un congruo termine per adempiere. Decorso questo termine senza adempiere, il contratto si considera risolto di diritto.

È importante notare che l'effetto della risoluzione contrattuale è retroattivo tra le parti, come indicato nell'articolo 1458, che sancisce gli effetti della risoluzione.

La risoluzione del contratto per inadempimento ha effetto retroattivo tra le parti, salvo il caso di contratti ad esecuzione continuata o periodica, riguardo ai quali l'effetto della risoluzione non si estende alle prestazioni già eseguite. Ciò significa che le prestazioni ricevute devono essere restituite, o reintegrate mediante un corrispettivo monetario nel caso in cui non siano restituibili, assicurando in tal modo che le parti ritornino allo status quo ante dopo la risoluzione del contratto. I casi sono tre: sono tre: I) la presenza di un contratto con attribuzioni corrispettive; II) l'inadempimento, quando esso presenti i seguenti due caratteri: a) sia imputabile, b) sia grave; III) l'attore in risoluzione deve avere eseguita la sua prestazione o dev'essere pronto ad eseguirla.

Mentre, il diritto di recesso consente alle aziende clienti di revocare unilateralmente un contratto entro un periodo di tempo specificato, senza dover fornire una motivazione specifica. Nel contesto dei contratti cloud, questo può avvenire per varie ragioni, come un cambio di esigenze da parte del cliente o un'insoddisfazione con i servizi offerti.

Secondo l'art. 1671 c.c., è prevista la fattispecie del recesso unilaterale dal contratto, secondo il quale il committente può recedere dal contratto, anche se è stata iniziata l'esecuzione dell'opera o la prestazione del servizio, purché vengano risarcite le spese sostenute e il mancato guadagno del fornitore.

D'altra parte, l'articolo 1373 disciplina il recesso convenzionale, che può essere liberamente convenuto dalle parti contrattuali. Tale facoltà può essere esercitata fino al momento in cui il contratto non abbia avuto un principio di esecuzione ¹⁵⁵. Tuttavia, nei contratti a esecuzione continuata o periodica, il recesso convenzionale non ha effetto sulle prestazioni già eseguite o in corso di esecuzione, garantendo così una certa continuità nelle relazioni contrattuali.

Il fornitore, in molti casi, si riserva il diritto di recedere unilateralmente dal contratto in qualsiasi momento, stabilendo un periodo di preavviso specifico nelle clausole contrattuali. Al termine di questo periodo, il fornitore avrà il diritto di disattivare i servizi senza ulteriori

¹⁵⁵<https://avvocato360.it/news/diritto-di-recesso-quando-si-puo-esercitare>

avvisi. E sarà compito del cliente assicurarsi di effettuare il backup dei propri dati prima che i servizi vengano disattivati ¹⁵⁶.

Nello specifico vi è la possibilità di ricorrere a:

- **Migration** ¹⁵⁷ – È essenziale prevedere la possibilità di migrare le proprie applicazioni verso un altro fornitore *Cloud* in modo chiaro e sicuro. Questo implica stabilire in modo predeterminato le modalità e tempistiche di uscita dal servizio *Cloud*, le modalità di restituzione dei dati e la garanzia di lasciare le interfacce di interoperabilità aperte, in modo da poter effettuare le operazioni di migrazioni in autonomia. La mancata regolazione della portabilità dei dati e dei tempi di uscita dal contratto di cloud rischia infatti di creare il c.d. *lock in*, cioè l'impossibilità di fatto di cambiare il provider. Sono rilevanti non solo però gli aspetti contrattuali, ma anche quelli tecnologici quali l'interoperabilità e la cancellazione dei dati.
- **Legge applicabile e foro competente in caso di controversie** – Nel caso in cui l'utente sia un'azienda valgono le clausole che limitano la responsabilità del Cloud provider, tra queste rientrano le clausole derogatorie, come ad esempio la clausola vessatoria.

3.4 L'azienda cliente: valutazione e scelta del cloud provider

Dallo scenario delineato nei paragrafi precedenti emerge che lo scenario contrattuale a cui il cliente è esposto è estremamente variegato, e pertanto, nella selezione di un fornitore deve tener conto di numerosi fattori. Elementi come le garanzie di *up-time*, le performance, la conformità alle normative sul tema del trattamento dei dati ecc. risultano essere fattori determinanti per l'azienda cliente. Occorrono in primis, come già evidenziato precedentemente, degli SLA adeguati alle esigenze dell'organizzazione aziendale. Il fatto che il *provider* offra la garanzia di continuità del servizio e la totale disponibilità dei dati rappresenta forse il primo parametro di comparazione quando un'azienda cliente si ritrova ad analizzare diverse offerte dai diversi *competitors* ¹⁵⁸.

¹⁵⁶<https://www.keliweb.it/tos.php>

¹⁵⁷<https://en.iusintech.com/il-contratto-di-cloud-computing/>

¹⁵⁸<https://www.digital4.biz/executive/guida-alla-scelta-del-cloud-provider-aspetti-da-valutare/>

Il profilo dei livelli di servizio sancito nel contratto di adesione deve tutelare l'azienda, e per questo servono delle clausole ad hoc. Saranno proprio i meccanismi di monitoraggio che consentiranno di valutare e comprovare lo stesso SLA. Se è ormai assodato che i Cloud provider, sono in grado di offrire al mercato livelli di sicurezza superiori a quelli di un data center proprietario, è ancora necessario fare delle distinzioni rispetto al tema della residenza dei dati ¹⁵⁹ ¹⁶⁰. Molti *player* si avvalgono di catene di fornitura diramati nel mondo; quindi, è importante privilegiare chi conserva ed elabora i dati esclusivamente in appositi hub che si trovano nell'Unione europea.

Il passaggio di un'infrastruttura tecnica da una configurazione *on-premise* al Cloud è determinato molto spesso da esigenze di scalabilità. L'idea proprio di "tecnologia applicata al Cloud" ¹⁶¹ sembra troppo vasto, anche se si restringe l'analisi solo alla scalabilità. Secondo quanto richiesto dall'utente, nel contesto Cloud scalabile, risorse come la capacità di calcolo, lo storage e larghezza di banda possono essere subito rilasciate e ciò deve avvenire sempre in modo dinamico e in base al *workload* ¹⁶², garantendo un miglioramento dei costi. Grazie all'allocazione dinamica delle risorse, esse possono essere incrementate o ridotte a *Runtime* in base alle fluttuazioni di traffico corrente.

L'elasticità è anche garantita dall'esistenza di politiche basate su metriche specifiche che fungono da riferimento per lo Scaling Automatico. Le metriche riguardanti la CPU ¹⁶³ o il numero di richieste/query al secondo sono rilevanti per la definizione di politiche e regole per l'automatizzazione dello Scaling. Quando superano o non raggiungono le soglie predefinite, il sistema può ridefinirle per adattarle al *workload* in esame. Per questo una piattaforma Cloud è anche una soluzione in grado di supportare la redistribuzione dei carichi per garantire la continuità di servizio e l'integrità delle informazioni gestite.

¹⁵⁹ L. SCHIAVINA, "Intelligenza artificiale e soft computing", 2019.

¹⁶⁰ <https://www.digital4.biz/executive/guida-alla-scelta-del-cloud-provider-aspetti-da-valutare/>

¹⁶¹ S. HURWITZ, "Cloud computing", 2020.

¹⁶² Un workload è la quantità di tempo e di risorse di calcolo che un sistema o una rete impiega per completare un'attività o generare un particolare output. Si riferisce alla domanda totale di sistema di tutti gli utenti e i processi in un momento specifico (<https://www.ibm.com/it-it/topics/workload>).

¹⁶³ Consiste nella componente di un calcolatore (detta anche processore) che carica le istruzioni dei programmi in memoria, le interpreta e manipola i dati di conseguenza (<https://www.treccani.it/enciclopedia/cpu/>).

Per l'orchestrazione, invece, si fa riferimento alla gestione coordinata e automatizzata di risorse e servizi nel Cloud. L'orchestrazione e l'automazione permettono di gestire insieme le risorse e di distribuire nuove istanze in base ad esigenze che si modificano nel tempo. Questo porta un aumento dell'efficienza operativa e a una scalabilità rapida e flessibile.

Il più grande vantaggio di tali tecnologie Cloud riguarda il fatto che, una volta completata la fase di integrazione dei sistemi, l'esecuzione manuale dei task viene ridotta al minimo. Questo beneficio è valido anche per pratiche DevOps e di CI/CD ¹⁶⁴, che consentono di velocizzare il rilascio di servizi e piattaforme. Gli strumenti e processi che consentono di attuare velocemente nuovi aggiornamenti e *bugfix* nel Cloud sono cruciali per ottimizzare l'efficienza operativa e la flessibilità.

Nel contesto Cloud la pianificazione automatica si ricollega ai concetti di efficienza e di adattabilità. In primis, si fa sempre affidamento al monitoraggio delle risorse che comprende sia la raccolta dei dati sull'impiego di risorse, quali CPU, storage, memoria RAM e larghezza di banda, che la loro analisi. Successivamente, le decisioni sulla distribuzione e l'allocazione delle risorse vengono generate automaticamente, a partire dai dati raccolti e analizzati durante il monitoraggio. Anche le politiche di bilanciamento del *workload*, la disponibilità delle risorse, i livelli di priorità delle applicazioni eseguite in Cloud, insieme ai livelli minimi di risorse disponibili per il funzionamento delle applicazioni critiche, sono aspetti rilevanti ¹⁶⁵. Il fine è garantire una scalabilità elevata anche quando si devono gestire svariati servizi come *Virtual Machine*, *Container* e database, che necessitano di un approccio flessibile alla pianificazione.

Spesso i fornitori di servizi ICT hanno solo provveduto a spostare sistemi informativi *on-premise* su servizi in cloud senza effettuare assesment di sicurezza per ridurre il *cyber risk*, rendendo le banche dati e i servizi digitali esposti sul cloud estremamente vulnerabili. Il fatto che si è passati dai sistemi informativi *on-premise* ai servizi *cloud* ha rappresentato un

¹⁶⁴ DevOps è un insieme di processi e strumenti automatizzati che consente agli sviluppatori e ai professionisti delle operazioni di collaborare in modo coeso alla creazione e alla distribuzione di codice in un ambiente di produzione (<https://www.atlassian.com/it/devops/devops-tools/devops-pipeline>).

¹⁶⁵ Cardarelli F., Amministrazione digitale, trasparenza e principio di legalità, in dir. Informaz. Informatica, 2014, pp. 211 ss.

nuovo approccio non solo nella definizione degli accordi sul livello di servizio, ma anche nel monitoraggio delle performance di sicurezza dei cloud service provider, avendo come conseguenza la creazione di una relazione di *Trust* tra fornitori e clienti ¹⁶⁶. La fiducia consiste nel ritenere che il fornitore gestirà in modo costruttivo la sicurezza nell'interesse del cliente ¹⁶⁷.

Un framework per la creazione e la gestione degli SLA porterebbe un livello idoneo di qualità e utilità negli SLA, basandosi sul concetto di *capability maturity* ¹⁶⁸. Si può concludere che ogni fase contiene processi distinti e che le fasi sono tutte interconnesse.

Tutti questi aspetti non devono essere considerati come mere peculiarità dei servizi cloud ma, sulla base di quanto analizzato precedentemente e sulla base delle criticità che possono emergere, è necessario che un cliente valuti tutti questi dettagli prima di procedere con la scelta di un fornitore. Nei paragrafi precedenti si è appunto parlato di contratti, capitolati, documenti tecnici e così via, dove il cliente può stabilire tutti gli elementi essenziali del servizio come la presenza di SLA, penali, previsione dei danni (quali danni d'immagine, mancati ricavi e tariffa oraria personale consumata inutilmente) e termini di decadenza per determinate fattispecie.

Attraverso questi meccanismi, il cliente può avanzare le giuste pretese nei confronti del fornitore prescelto ed evitare le contingenze che tipicamente comportano il sostenimento di costi extra budget che ledono, ulteriormente, l'azienda nel caso di inadempienza da parte del CSP.

Al fine di avere un riscontro concreto rispetto a quanto analizzato, per capire nel concreto quelli che sono gli elementi che un'azienda deve valutare è possibile esaminare delle clausole specifiche di un contratto cloud, quale ad esempio quello previsto per l'implementazione di

¹⁶⁶ <https://www.vincenzocalabro.it/article/2024/minacce-e-vulnerabilita-del-cloud-computing-come-proteggersi.html>

¹⁶⁷ <https://www.agendadigitale.eu/cultura-digitale/aria-agcom-la-complessa-mission-dellautorita-nellattuale-mosaico-digitale/>

¹⁶⁸ Il Capability Maturity Model Integration (CMMI) è un modello che consente di migliorare la maturità dei processi orientato allo sviluppo di prodotti e servizi e può essere utilizzato come guida per il miglioramento di processi sia nell'ambito di gestione dei progetti sia in quello di un'intera organizzazione (<https://www.dnv.it/services/capability-maturity-model-integration-cmmi--143843/>).

SAP in cloud¹⁶⁹ ed anche per quello di AWS ¹⁷⁰.

In primis, è necessario analizzare quello che è il contenuto del contratto in oggetto. Ciò che viene messo in luce sono i termini del servizio, fondamentali per definire l'ambito giuridico e le attività specificando ai clienti come possano accedere ai servizi offerti. Tanto è vero che nella prassi l'ambito e quindi i termini del servizio sono utili a definire il perimetro del progetto di implementazione. Rispetto a questi servizi, infatti, l'attenzione va posta sulla modifica degli stessi che può rappresentare infatti un rischio per il cliente. La clausola, presente sia da parte di SAP che AWS, tuttavia definisce due possibili scenari. Ad esempio, AWS si riserva il diritto di modificare i suoi servizi in qualsiasi momento. Tuttavia, AWS cerca di garantire che le modifiche non abbiano un impatto negativo significativo sui clienti. Questo in genere può risultare rischioso se, a seguito di una particolare condizione modificata, il cliente si trovi in oggettiva difficoltà operativa. Invece SAP, da questo punto di vista, si mostra essere nuovamente flessibile prevedendo all'interno dei suoi contratti la possibilità di un consenso reciproco e negoziabile prima di effettuare una qualsiasi variazione contrattuale. Questi elementi possono essere gestiti con l'attivazione di servizi aggiuntivi, quali ad esempio delle garanzie oppure un servizio di manutenzione della piattaforma¹⁷¹.

Altro elemento sono le condizioni di pagamento. Generalmente su queste vi è anche l'appoggio, per una specifica valutazione, sia dell'ufficio acquisti che dell'ufficio contabilità di un'azienda cliente in quanto si vanno a definire le cosiddette milestones di progetto ovvero momenti di consegna di lavoro che danno diritto al provider di riscuotere quota parte del canone pattuito in seno al contratto.

Un elemento fondamentale del contratto è la garanzia. SAP garantisce infatti nel suo contratto per un periodo di sei mesi dalla consegna del Software, il Software sarà sostanzialmente conforme alla descrizione funzionale riportata nella documentazione standard; questo è un elemento fondamentale in quanto come analizzato precedentemente, l'adozione di un sistema

¹⁶⁹ <https://assets.cdn.sap.com/agreements/data-processing-agreements/tom/technical-and-organizational-measures-toms--sap-cloud-services-italian-v12-2021.pdf>

¹⁷⁰ [https://d1.awsstatic.com/legal/aws-customer-agreement/AWS%20Customer%20Agreement_Italian_%20\(2023-10-27\).pdf](https://d1.awsstatic.com/legal/aws-customer-agreement/AWS%20Customer%20Agreement_Italian_%20(2023-10-27).pdf)

¹⁷¹ <https://cmmsitalia.it/software-manutenzione-in-cloud/>

cloud implica quello che nel gergo è riconosciuto come change management ¹⁷² quindi un cambiamento che l'azienda si ritrova a gestire e, senza garanzie a supporto, rischia di generare delle perdite operative ed economiche di non poco conto.

Altro aspetto fondamentale riportato nella definizione del contratto ¹⁷³, è quello dell'assunzione di responsabilità del provider nella gestione dei dati, tema delicato affrontato con l'articolo 29 sul cloud computing. Infatti, il provider SAP si impegna ad attivare delle operazioni di backup periodico al fine di storare correttamente tutti i dati transazionali inseriti sulla piattaforma preservandone l'accessibilità e l'integrità. Infatti, sempre in una clausola dedicata, definisce anche che l'accessibilità dei dati viene affidata al solo cliente con il quale viene stipulato il contratto.

Altro aspetto fondamentale che, nella prassi commerciale è affrontato, è quello della delimitazione al servizio inteso come offerta in termini di manutenzione del sistema. Tipicamente i provider, infatti, devono prevedere anche dei servizi di AMS (Application Management Service) che consentano al cliente di avere un ulteriore supporto funzionale e tecnico post implementazione di un sistema cloud. Questo aspetto deve essere previsto sempre in ottica di change affinché l'azienda si impegni con il provider a tutelare la propria operatività.

Passando invece a quanto previsto da AWS ¹⁷⁴, nei loro contratti è possibile notare che le clausole in termini di responsabilità sono ben predefinite. Questo è il contratto standard che copre la maggior parte dei servizi AWS. È progettato per essere utilizzato da una vasta gamma di clienti senza modifiche significative. Nel contratto è possibile anche notare come si pone l'attenzione sulle SLA ¹⁷⁵, altro elemento fondamentale per la buona riuscita di un progetto. AWS fornisce SLA per molti dei suoi servizi, che garantiscono un certo livello di

¹⁷² Il change management nei contratti cloud si riferisce alla gestione delle modifiche contrattuali e operative che possono verificarsi durante la durata di un accordo per servizi cloud. Questo processo è fondamentale per garantire che tutte le parti coinvolte comprendano e accettino eventuali cambiamenti nelle condizioni del contratto o nei servizi forniti.

¹⁷³ <https://assets.cdn.sap.com/agreements/data-processing-agreements/tom/technical-and-organizational-measures-toms--sap-cloud-services-italian-v12-2021.pdf>

¹⁷⁴ [https://d1.awsstatic.com/legal/aws-customer-agreement/AWS%20Customer%20Agreement_Italian_%20\(2023-10-27\).pdf](https://d1.awsstatic.com/legal/aws-customer-agreement/AWS%20Customer%20Agreement_Italian_%20(2023-10-27).pdf)

¹⁷⁵ <https://aws.amazon.com/legal/service-agreements-level>

disponibilità. Ad esempio, l'SLA per Amazon EC2 ¹⁷⁶ garantisce una disponibilità del 99,99% su base annuale. Inoltre, se AWS non riesce a rispettare gli SLA, i clienti possono avere diritto a crediti di servizio come forma di rimborso rendendo così meno oneroso il mancato adempimento da parte del provider. Invece SAP, per la gestione delle SLA, mostra un maggior grado di flessibilità consentendo all'azienda di definire quelli che sono i profili necessari alla definizione del limite temporale nel quale risolvere una determinata criticità.

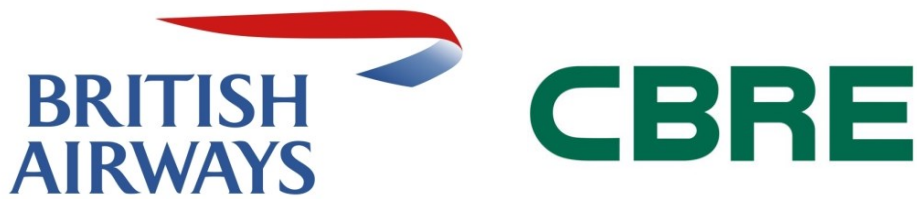
Volendo analizzare anche quelli che sono i rischi per il cliente, dall'analisi dei contratti, è possibile evidenziare:

- Dipendenza dal Fornitore: Essere legati a un unico fornitore di servizi cloud può comportare rischi in termini di lock-in tecnologico e aumento dei costi nel tempo. Questo può valere per entrambi i provider in quanto fornendo delle specifiche piattaforme di proprietà questo può rendere difficile organizzare una migrazione in quanto sovente i sistemi non risultano integrati tra loro ed è quindi necessario attivare altre forniture per l'organizzazione di una data migration.
- Sicurezza dei Dati: Anche se entrambi i provider offrono robusti meccanismi di sicurezza, la responsabilità finale della protezione dei dati resta in parte del cliente, specialmente nella configurazione e gestione delle risorse.
- Costi Variabili: La struttura dei costi di AWS è basata sull'uso effettivo, il che può portare a spese impreviste se non attentamente monitorate e gestite. Stesso discorso anche per SAP.

Questo confronto, seppur limitato a delle clausole ben specifiche, evidenzia come AWS e SAP adottino approcci differenti per i contratti cloud, con AWS che offre maggiore flessibilità e standardizzazione, mentre SAP tende a personalizzare maggiormente i contratti in base alle esigenze specifiche dei clienti aziendali. Entrambi i fornitori pongono grande enfasi sulla sicurezza, la conformità e il supporto tecnico, ma le modalità di implementazione e gestione

¹⁷⁶ https://docs.aws.amazon.com/it_it/AWSEC2/latest/UserGuide/concepts.html

possono variare significativamente e, di conseguenza, generando diversi impatti sull'azienda cliente.



4.1 Contesto del caso: British Airways vs CBRE

Al fine di comprendere l'effettiva applicazione del modello del cloud computing nella realtà aziendale e contrattuale, in questo capitolo viene analizzato tale modello nell'industria dell'aviazione, andando ad esaminare il rapporto intercorrente tra due grandi aziende: la British Airways e la CBRE.

British Airways è una compagnia aerea del Regno Unito con sede a Hillingdon, il borgo più occidentale di Londra, vicino al suo hub principale, l'aeroporto di Londra-Heathrow ¹⁷⁷. È la più grande compagnia aerea britannica per flotta, voli e numero di destinazioni internazionali e la seconda per numero di passeggeri trasportati.

CB Richard Ellis (CBRE), invece, è una società leader a livello internazionale nel settore del real estate ¹⁷⁸. Con oltre un secolo di esperienza e 800 data center in gestione, offre servizi di consulenza e investimenti nel settore immobiliare commerciale. Grazie ai suoi servizi, insight e dati che coprono ogni dimensione del settore, CBRE si pone l'obiettivo di creare soluzioni per clienti di ogni genere, tipologia e localizzazione, aiutandoli a gestire i propri asset e a dare nuova vita al proprio business.

Nel 2003, British Airways aveva stipulato un contratto con CBRE per gestire il suo portafoglio immobiliare globale di 8,5 milioni di piedi quadrati (circa 790.000 m²), di cui oltre 7 milioni di piedi quadrati nel Regno Unito ¹⁷⁹. L'accordo concluso tra le due grandi società prevedeva che il Global Corporate Services di CBRE fornisse a British Airways, oltre al già menzionato obiettivo, anche un servizio di consulenza per rendere più efficiente l'utilizzo

¹⁷⁷ https://it.wikipedia.org/wiki/British_Airways

¹⁷⁸ Attività che si occupa in toto della gestione, della compravendita e della valorizzazione degli immobili.

¹⁷⁹ [CBRE nominata per la gestione del patrimonio globale di British Airways \(europe-re.com\)](http://europe-re.com)

della proprietà e per potenziare i servizi di gestione del progetto di design, sviluppo e localizzazione degli edifici.

CBRE, inoltre, si occupava della gestione delle transazioni per British Airways, oltre che dei data center della società aeroportuale nel London Heathrow. In questo modo, British Airways dimostrava di possedere un approccio innovativo nell'uso della proprietà che le avrebbe garantito la leadership per l'industria dell'aviazione.

Questa collaborazione portò a una crescita tale per CBRE da garantirsi la nomina per la valutazione del portafoglio del Regno Unito dal 2010 al 2015.

4.2 Il ruolo del cloud computing nell'industria dell'aviazione

Il *cloud computing* ha rivoluzionato il sistema dell'aviazione. Questa tecnologia si sta sempre più diffondendo tra le compagnie aeree, le quali la adottano per aumentare l'efficienza, migliorare l'esperienza dei passeggeri e ridurre i costi.

1. Per quanto attiene **l'efficienza operativa**, il sistema del cloud consente di archiviare i dati sugli orari degli aeromobili, dell'equipaggio e dei passeggeri, ai quali può accedere in tempo reale tutto il personale interessato. Ciò permette un miglior coordinamento delle attività e riduce la probabilità di conflitti di pianificazione. Inoltre, le compagnie aeree possono utilizzare un software basato su cloud per gestire i programmi di manutenzione e riparazione, il che può aiutare a ridurre i tempi di inattività e aumentare la disponibilità degli aeromobili.
2. Questo approccio tecnologico, inoltre, può essere utilizzato per garantire una **miglior esperienza di volo ai passeggeri**, consentendo alla compagnia aerea di fornire ai passeggeri l'accesso all'intrattenimento (musica, film e programmi TV) basato su cloud, particolarmente importante su lunghe tratte. In più, consente un'evoluzione dalle consuete pratiche di messaggistica istantanea e aggiornamenti in tempo reale ai dipendenti ed ai clienti, fornendo rapidamente le informazioni necessarie tramite

applicazioni sui dispositivi mobili e su qualsiasi tipo di sistema operativo ¹⁸⁰. Ciò contribuisce ad evitare problematiche scaturite dallo stato del volo, dai ritardi e dai cambi di gate ¹⁸¹.

Assicurando tutti questi comfort al passeggero, le aziende dell'aviazione investono al fine di essere scelti sia da clienti che viaggiano per piacere e svago, sia dai clienti che lo fanno per motivi lavorativi.

3. Un altro aspetto molto importante è sicuramente quello economico, in quanto il cloud computing aiuta ad abbattere i costi. Gestendo completamente l'hardware che esegue le applicazioni, con una potenza di calcolo scalabile in base alle esigenze aziendali fluttuanti, il cloud riduce la necessità di infrastrutture hardware e software costose. Inoltre, semplifica l'implementazione del software, facilita il percorso di migrazione per il trasferimento al cloud, e riduce i requisiti di manutenzione, contribuendo a ridurre il costo totale di proprietà nel processo ¹⁸².

Un'altra sfida che gli aeroporti devono affrontare è la necessità di cooperare insieme su scala globale: gli aeroporti, le compagnie aeree e gli agenti di Handling devono lavorare insieme per massimizzare i tempi di rotazione degli aeromobili. È anche importante collaborare con le agenzie di sicurezza delle frontiere per la protezione i dati biometrici privati dei passeggeri. Con il *cloud computing* è possibile l'accesso ai dati, ma al contempo garantisce la proprietà, il controllo e la privacy di questi ¹⁸³.

Il modello cloud ha innovato anche il metodo di pagamento, consentendo di pagare in modo semplice e sicuro con la tecnologia contactless per servizi aggiuntivi come i bagagli o l'accesso ai lounge presso tutti i banchi del check-in.

Inoltre, migliora la sicurezza nel settore dell'aviazione grazie al cloud, poiché consente l'utilizzo di sistemi per l'archiviazione e l'analisi dei dati provenienti dai sensori degli

¹⁸⁰ https://www.linkedin.com/pulse/cloud-skies-scope-computing-aviation-industry-rajat-nayar?trk=portfolio_article-card_title

¹⁸¹ <https://www.aviationfile.com/cloud-computing-in-aviation/>

¹⁸² <https://www.nutanix.com/it/info/what-is-hybrid-cloud>

¹⁸³ <https://www.forbes.com/sites/forbestechcouncil/2022/03/03/how-cloud-technology-can-enhance-your-airport-experience/>

aeromobili, impiegati per identificare potenziali rischi per la sicurezza prima che diventino critici. La tecnologia cloud può migliorare questo aspetto in diversi modi. Ad esempio, gli aeroporti possono gestire con attenzione la sicurezza delle piste (includendo controlli regolari sulla presenza di animali e detriti), così come la sicurezza dei bagagli, la sicurezza delle strutture e la manutenzione e la protezione degli aeromobili. Quindi il cloud computing diventerebbe di vitale importanza per tracciare accuratamente gli aeromobili in tempo reale, indipendentemente dalle apparecchiature di tracciamento standard che potrebbero essere disabilitate sugli aeromobili ¹⁸⁴.

Le soluzioni di *cloud computing* potrebbero, altresì, offrire un'accelerazione dei processi di manutenzione degli aeromobili e facilitare la conservazione e il trasferimento dei dati degli aerei in caso di incidente. Questo sarebbe reso possibile grazie allo spazio di archiviazione e ai fattori post-incidente, come l'impatto o l'esposizione all'ambiente, ampliando così la portata delle scatole nere attualmente in uso, che sono limitate nel tempo.

Infine, i sistemi basati su cloud sono preziosi poiché riescono a fornire ai piloti informazioni meteorologiche in tempo reale, aiutandoli ad evitare turbolenze e altri pericoli legati alle condizioni meteorologiche ¹⁸⁵.

È in questo contesto evolutivo che si inserisce l'adesione da parte di British Airways a questa innovativa tecnologia proposta e curata da CBRE.

4.3 Il cloud computing in British Airways

Come già accennato nel primo paragrafo, British Airways è una compagnia aerea inglese la cui fondazione risale al 1971, dalla fusione delle due principali compagnie aeree britanniche del tempo, BOAC e British European Airways, più altre due piccole compagnie aeree regionali, Cambrian Airways e Northeast Airlines. Già nel 1976 assunse l'esclusiva gestione dei voli internazionali verso il Nord America e il Sud-Est asiatico dalla rivale britannica

¹⁸⁴ https://www.linkedin.com/pulse/cloud-skies-scope-computing-aviation-industry-rajat-nayar?trk=portfolio_article-card_title

¹⁸⁵ <https://www.ibm.com/it-it/topics/cloud-computing-benefits>

Caledonian. Nel corso degli anni, incorporò altre compagnie e nel 1987, parte della compagnia fu privatizzata e quotata alla Borsa di Londra, processo che la portò ad una rapida crescita. Nonostante periodi di crisi finanziaria dovuti a scelte aziendali azzardate e remunerative, agli inizi degli anni 2000, grazie alla fusione con la compagnia spagnola Iberia e alla cooperazione con American Airlines, nacque l'International Airlines Group (IAG), gruppo che vanta oltre 400 aeromobili e vola verso oltre 200 destinazioni in tutto il mondo.

L'espansione repentina ha portato i vertici a considerare modi sempre più all'avanguardia per l'organizzazione e la gestione dell'intera azienda.

Prima di optare per l'utilizzo del cloud e concludere un accordo con CBRE, British Airways utilizzava un programma di premi per i soci che si iscrivevano al loro Executive Club. Grazie all'accumulo di Avios, la valuta del Club, volando con British Airways e i partner, i clienti potevano ottenere sconti, soggiorni in hotel gratuiti, noleggi auto e altro ancora. Il suddetto programma aveva diversi livelli di adesione e in base alla partecipazione ad uno di esso dipendevano i vantaggi e i servizi offerti all'abbonato. Per esempio, i membri Gold e Platinum avevano priorità di imbarco, consentendo loro di salire a bordo prima degli altri passeggeri.

Successivamente, British Airways, aderendo al processo evolutivo informatico, cercò di migliorare l'efficienza operativa riducendo i costi e ottimizzando le risorse. A tal fine, risultò necessario includere l'implementazione di nuove tecnologie, l'ottimizzazione delle rotte e la gestione efficiente del personale. L'azienda decise quindi di investire, così come continua a fare, in soluzioni digitali per migliorare l'esperienza del cliente e semplificare le operazioni.

Il primo passo verso la modernizzazione digitale risale al 2003, anno in cui la British Airways concluse un accordo con l'azienda CBRE che utilizza il cloud computing, tecnologia in continua evoluzione che alimenta servizi ed applicazioni online e permette l'utilizzazione di spazi di archiviazione, software e programmi vari. Come si è già esaminato, i vantaggi del cloud per le compagnie aeree sono molteplici e contribuiscono a garantire un servizio completo per i viaggiatori e in toto al lavoro dell'industria dell'aviazione.

Negli anni, British Airways ha collaborato anche con altre aziende competenti in materia di

cloud, come la Juniper Networks nel 2015 ¹⁸⁶. La partnership con quest'ultima era volta alla costruzione di un data center cloud privato e una dorsale core IP/MPLS12, con lo scopo di supportare applicazioni quali l'emissione di biglietti, il check-in e il monitoraggio dei bagagli. Per questa collaborazione informatica, la scelta della British Airways fu proiettata all'utilizzo dell'architettura MetaFabric di Juniper Networks nella nuova struttura, che comprende il sistema QFabric di Juniper e gli switch Ethernet della serie EX ¹⁸⁷. Secondo l'azienda, l'utilizzo di questa tecnologia avrebbe aiutato a scalare facilmente il data center anche con l'evoluzione nel tempo esigenze IT.

La British Airways ha cooperato anche con la Microsoft per implementare il servizio di assistenza clienti a bordo abilitato per il Wi-Fi. Il sistema consente ai teams di assistenza a terra di comunicare con l'equipaggio di cabina e risolvere i problemi prima dell'arrivo dei voli.

Il processo di digitalizzazione per la British Airways non si è ancora arrestato, in quanto di recente ha stanziato un programma di modernizzazione da 9 miliardi di dollari per il trasferimento di 700 sistemi nel cloud, senza rivelare però a quale azienda si affiderà.

4.4 CBRE: il servizio di cloud computing

La leader mondiale dell'innovazione scientifica CBRE utilizza da sempre *macchine virtuali* alimentate dal cloud, così da poter gestire il proprio patrimonio aziendale in itinere. Il cloud e i datacenter stanno diventando sempre più fondamentali per le aziende e gli investitori, e proprio la CBRE è al centro di questa evoluzione digitale. Utilizzando dati su larga scala e tecnologie di livello enterprise, CBRE si pone l'obiettivo di creare soluzioni immobiliari all'avanguardia.

Le start-up che adottano questo tipo di tecnologia sono in grado di eliminare le spese generali

¹⁸⁶ [British Airways private cloud takes flight with Juniper Networks | ITPro](#)

¹⁸⁷ **MetaFabric di Juniper Networks:** Architettura di rete progettata per semplificare la gestione dei data center, migliorandone flessibilità, scalabilità e prestazioni.

QFabric di Juniper Networks: Sistema di rete che combina diverse funzioni in un'unica piattaforma, riducendo la complessità e i costi.

Switch Ethernet della serie EX di Juniper Networks: Dispositivi di rete che offrono connessioni veloci e affidabili per data center e reti aziendali.

e i costi di apertura degli uffici, soprattutto in città dove gli immobili sono costosi. Come già evidenziato, CBRE collabora anche con le compagnie aeree, vantando un team di esperti e la conoscenza delle condizioni del mercato locale per fornire consulenza leader del settore, risultati strategici e transazionali. Fornisce una gamma completa di servizi immobiliari commerciali per l'industria aerospaziale, inclusi aeroporti, compagnie aeree, ambienti aerospaziali e di difesa, MRO, produzione critica e linee di assemblaggio finale ¹⁸⁸.

Il team Aviation dell'azienda si concentra in particolare sulla fornitura di servizi di *Facility Management*, ovvero la produzione di tutti i servizi fondamentali per la gestione operativa e strategica delle aziende. Questi servizi mirano a migliorare le performance dei dipendenti, mettendo a loro disposizione un ambiente di lavoro atto a soddisfare i bisogni professionali ma soprattutto conforme alle norme in materia di salute, sicurezza e ambiente ¹⁸⁹.

CBRE offre servizi soft attraverso partner affidabili e considerati i migliori nel settore, assicurando manutenzione meccanica ed elettrica, pulizia, sicurezza, gestione dei rifiuti e controllo dei parassiti per tutti gli ambienti dell'aviazione, inclusi uffici, hangar, lounge, terminal e linee di assemblaggio finale ¹⁹⁰. Per British Airways, l'azienda gestiva perfino il portafoglio immobiliare globale, ovvero i terreni e le strutture possedute dalla compagnia aerea, con l'obiettivo di amministrare le strutture già realizzate ed edificate sui terreni ancora vuoti.

Nei paragrafi precedenti abbiamo analizzato i molteplici vantaggi del modello cloud, ma, sebbene siano poche, non mancano alcune note negative derivanti dall'utilizzo di questa tecnologia. Dapprima, appare opportuno analizzare l'aspetto più importante: la gestione della privacy. I soggetti coinvolti sono principalmente il titolare, ovvero colui che decide le finalità e le modalità del trattamento dei dati, e il responsabile, che tratta i dati per conto del titolare ¹⁹¹. Il Regolamento Generale sulla Protezione dei Dati (GDPR) richiede che il titolare designi per iscritto il responsabile del trattamento tramite un contratto dedicato (Art. 28 Reg. 679/2016). La tutela contrattuale è di vitale importanza quando si utilizza un servizio di cloud

¹⁸⁸ <https://www.cbre.co.uk/services/industries/aviation>

¹⁸⁹ <https://www.appvizer.it/rivista/organizzazione/facility/facility-management>

¹⁹⁰ <https://www.cbre.co.uk/services/industries/aviation>

¹⁹¹ https://it.wikipedia.org/wiki/Cloud_computing

computing per memorizzare dati personali o sensibili, poiché l'utente si espone a potenziali problemi di violazione della privacy.

Molto spesso, i dati personali vengono memorizzati nelle *Server Farms*¹⁹² di aziende che risiedono in uno Stato diverso da quello dell'utente, sottraendo i dati ad un controllo accurato del cliente.

La sicurezza dei dati può essere affrontata sia dai *cloud provider* che dai loro clienti. Accade che il cloud provider non sia il proprietario dei server sui quali vengono fisicamente ospitati i dati, ma si affida a fornitori esterni di servizi di hosting. Difatti, secondo quanto stabilito dall'Art. 28 Reg. 679/2016, l'Hosting Provider, che gestisce i dati trasmessi dal *cloud provider* per conto del titolare, assume il ruolo di sub-responsabile del trattamento dei dati.

La conseguenza di questa operazione è che il *cloud provider* deve ottenere il consenso del titolare del trattamento per avvalersi di un sub-responsabile, al quale dovrà trasferire le istruzioni fornite dal titolare tramite il contratto di designazione del responsabile. In sostanza, il titolare del trattamento deve sempre mantenere il controllo dei propri dati e, per farlo, è opportuno comprendere l'intera catena di trattamento dei dati al fine di garantire la loro sicurezza. Il cloud provider deve fornire sistemi di crittografia sempre più raffinati, sebbene, se non diversamente concordato nel contratto, è un onere del cliente decidere di impiegarli.

Inoltre, come già anticipato nel capitolo precedente, le clausole del contratto di servizi in cloud prevedono che l'utente possa porre fine al servizio in qualsiasi momento e che il fornitore possa modificare unilateralmente il contratto, senza contraddittorio con l'utenza, fatta salva la possibilità per l'utente di recedere dal servizio. Con l'aumento della richiesta di servizi cloud da parte delle imprese, i provider propongono condizioni generali di contratto e termini di utilizzo con modalità unilaterali, legati sempre alla questione che la convenienza di queste piattaforme sta nell'alta standardizzazione delle offerte e dei sistemi previsti.

In tal senso, oltre al codice di condotta sul *cloud computing* approvato dal board dei garanti

¹⁹² Server collocati in un unico ambiente in modo da poterne centralizzare la gestione, la manutenzione e la sicurezza https://mydbook.giuntitvp.it/app/books/GT2024_G4554371A/pdf/16

dell'Unione Europea, la CBRE ha fatto redigere un “Codice di condotta dei fornitori”¹⁹³ nel quale, tra le altre cose, si impegna affinché “*i propri amministratori, funzionari, dipendenti, agenti, rappresentanti, fornitori, subappaltatori e altri partner aziendali comprendano e rispettino i requisiti stabiliti nel presente Codice*”. Inoltre, il fornitore dovrà informare prontamente per iscritto l'azienda in caso di violazione sospetta o verificata del presente Codice, incluse, senza limitazioni, le attività illegali o le violazioni dei diritti umani.

Per quanto riguarda la posizione geografica dei server, è necessario conoscere molto bene il luogo in cui vengono raccolti i dati, poiché è vietato trasferirli in paesi che non garantiscono un livello adeguato di protezione. Il luogo di permanenza dei dati può diventare un problema quando dati pubblici sono raccolti e conservati in archivi privati situati in un paese diverso da quello degli utenti, poiché spesso si tratta di produzioni di importanza cruciale, informazioni personali e contenuti intellettuali, e gli utenti non hanno garanzie di un libero accesso futuro a tali dati. Per garantire maggiore sicurezza, è preferibile che il fornitore di servizi cloud appartenga alla stessa nazione o area geografica del cliente, applicando le stesse leggi e normative sulla privacy e sicurezza. In caso contrario, CBRE ha stabilito che il fornitore è tenuto a informarla se ritiene che nel paese in cui opera o presta i suoi servizi vigano leggi (sia esistenti che sopravvenute a causa di modifiche normative) che impediscano la protezione dei dati o i termini del contratto di fornitura con CBRE, o che possano recare sostanziale pregiudizio a tale rispetto.

Come si vedrà nel paragrafo successivo, un'altra grave minaccia per la disponibilità nel *cloud computing* è la perdita accidentale di rete tra l'utente e il fornitore o il malfunzionamento del server causato da attacchi DoS (Denial of Service) distribuiti o altre azioni malevole. Un eventuale malfunzionamento, inoltre, colpirebbe un numero molto elevato di persone contemporaneamente, dato che questi sono servizi condivisi. Quindi, la riuscita della prestazione dei servizi di cloud computing si affida alla disponibilità di una connessione Internet ad alta velocità per il download e upload dei dati. Qualora si dovesse verificare un'interruzione nella connessione dovuta al proprio *Internet Service Provider* (ISP), tutte le attività che richiedono l'accesso al cloud potrebbero paralizzarsi e questo può avere un impatto

¹⁹³ [cbre-supplier-code-of-conduct-italian.pdf](#)

significativo sulle operazioni aziendali o sulle attività personali degli utenti. A causa delle lacune normative e delle già menzionate clausole di esclusione di responsabilità del *cloud provider*, l'azienda che riceve il servizio cloud, nel caso in cui ci fosse l'interruzione del servizio, non sarebbe tutelata come dovrebbe.

Infine, occorre sottolineare che la CBRE nel codice di fornitura non s'impegna in alcun modo a monitorare o verificare il rispetto del codice stesso, ma prevede come unico responsabile il fornitore del servizio. Tuttavia, il fornitore è tenuto a consentire a CBRE e/o ai suoi rappresentanti di valutare la sua conformità quando offre servizi o fornisce prodotti a CBRE. Le valutazioni possono includere, senza limitazioni, l'ispezione in loco delle strutture del fornitore e l'esame delle relative informazioni del fornitore per verificare il rispetto del codice di fornitura.

4.5 La Controversia British Airways vs CBRE

Nel maggio 2017, due dei data center inglesi gestiti dalla CBRE - Boadicea House e Comet House, situati vicino a Heathrow – hanno smesso di funzionare improvvisamente, causando circa 75.000 cancellazioni di prenotazione e più di 672 voli, causando caos negli aeroporti londinesi di Heathrow e Gatwick ¹⁹⁴. British Airways ha raggiunto un accordo legale con alcuni dei 420.000 individui colpiti dalla violazione dei dati, che ha interessato sia i clienti che il personale di British Airways e includeva nomi, indirizzi e dettagli delle carte di pagamento. L'Information Commissioner's Office (ICO) ha inflitto a British Airways la sua multa più grande fino a quel momento, pari a 20 milioni di sterline, per il "fallimento inaccettabile" nel proteggere i dati dei clienti.

L'interruzione ha interessato proprio l'intera gamma di operazioni di British Airways, comprese le prenotazioni, il check-in dei voli, i call center e l'app mobile. I problemi sono persistiti per tre giorni, probabilmente a causa di un guasto all'alimentazione.

Dopo le indagini, si è arrivati alla conclusione che la responsabilità dell'interruzione fosse di

¹⁹⁴ <https://europe-re.com/cbre-appointed-to-manage-british-airways-global-estate/24658>

CBRE, in qualità di gestore in *outsourcing* della struttura. Tuttavia, i funzionari dell'International Airlines Group hanno notato che l'impianto aveva perso energia per un breve periodo di tempo, ma soprattutto che il danno maggiore era stato scatenato dalla riattivazione dell'alimentazione non avvenuta secondo gli standard, causando uno sbalzo di tensione. Non è mai stato compreso il motivo per il quale il *failover* sull'altro data center della compagnia aerea nell'area non abbia funzionato: l'unico indizio per comprendere la gravità del problema si rinveniva in un'e-mail inviata al personale dal capo del gruppo IT di IAG, la quale attribuiva la responsabilità ad un soggetto che aveva ignorato un UPS, con conseguente "perdita totale e immediata di energia alla struttura, bypassando i generatori e le batterie di backup"¹⁹⁵. Tale errore non ha permesso la migrazione di emergenza controllata verso altre strutture.

Come precedentemente affermato, negli accordi tra aziende e cloud provider spesso vi è una limitazione o esclusione di responsabilità. Infatti, tali accordi prevedono l'esclusione / limitazione della responsabilità del cloud provider per ogni tipo di danno derivante dall'utilizzazione o dall'impossibilità di utilizzazione dei servizi oggetto di contratto, salvi i limiti inderogabili di legge¹⁹⁶. È comune trovare clausole di deresponsabilizzazione per il caso della perdita dei dati del cliente. E in questo caso, alcuni esperti hanno sostenuto che l'errore di sistema poteva essere ricondotto anche ad un problema di progettazione dei data center, oltre che alla loro strategia di *failover*, poiché nessun singolo errore sarebbe stato in grado di arrestare l'intero server.

Un anno e mezzo dopo l'evento, non essendo riusciti a trovare un accordo sulla causa principale dell'incidente, le due società si sono rivolte al tribunale. Tutt'oggi non si conoscono con certezza le effettive cause che hanno provocato il guasto, o a chi attribuire la responsabilità, dimostrando in tal senso che le interruzioni dei data center restano un argomento ostico da comprendere.

Successivamente ai fatti avvenuti nel 2017, ci sono state iniziative di settore per provare a facilitare le segnalazioni delle cause di guasto senza rivelare informazioni aziendali critiche,

¹⁹⁵ <https://www.datacenterknowledge.com/uptime/cbre-settles-british-airways-lawsuit-over-costly-data-center-outage>

¹⁹⁶ <https://www.zerounoweb.it/cloud-computing/contratti-cloud-le-clausole-da-tenere-d-occhio/#:~:text=In>

come per esempio il Data Center Incident Reporting Network (DCiRN), lanciato proprio nel giugno del 2017. L'idea alla base è simile a quello dell'Autorità per l'Aviazione Civile, che finanzia le indagini sugli incidenti aerei.

Infine, sebbene l'interruzione sia costata alla compagnia aerea 58 milioni di sterline (74,6 milioni di dollari) in richieste di risarcimento dei passeggeri, pare che la British Airways abbiano raggiunto un accordo senza ammissione di responsabilità con la CBRE, mantenendo il loro rapporto di collaborazione ¹⁹⁷.

¹⁹⁷ <https://www.computerweekly.com/news/252457343/British-Airways-settles-legal-claim-with-CBRE-over-May-2017-Bank-Holiday-datacentre-outage>

Conclusione

Alla luce dell'analisi svolta nei paragrafi precedenti e nella totalità del presente elaborato, è facile da notare che la progressione verso il cloud ha permesso la sperimentazione di servizi altamente efficienti e l'organizzazione intelligente di una forza lavoro ben distribuita. Sebbene il cloud abbia avuto una presenza in varie forme per circa 20 anni, l'evoluzione tecnologica ha arricchito questo servizio di vantaggi sia economici che funzionali. Il cloud pubblico ha rivoluzionato il modo in cui la tecnologia si evolve: l'intelligenza artificiale, i sistemi di contabilità, l'analisi dei dati e altri servizi costosi possono ora essere sperimentati a prezzi accessibili, consentendo la valutazione di diverse soluzioni. Inoltre, in passato, l'approvvigionamento di hardware e software richiedeva mesi, ma con i cloud pubblici è possibile valutare rapidamente se una soluzione offre un valore reale.

Abbiamo anche osservato che i servizi basati sul cloud tendono a svilupparsi con una velocità superiore, principalmente grazie alla prontezza dei feedback degli utenti e alla flessibilità dei fornitori nell'adottare metodologie di sviluppo agile e *DevOps*. Questo consente loro di risolvere rapidamente eventuali problematiche e di implementare nuove funzionalità richieste dagli utenti, rendendole disponibili quasi istantaneamente.

È evidente che grazie al cloud computing, la forza lavoro distribuita è diventata la norma. L'esplosione del lavoro remoto, accelerata dalla pandemia di COVID-19, ha dimostrato alle aziende il potenziale del cloud computing nel supportare una forza lavoro distribuita in modo flessibile ed efficiente. Prima del COVID-19, la tecnologia era principalmente utilizzata all'interno del firewall aziendale.

Inoltre, il cloud computing ha abbattuto i confini geografici, consentendo alle aziende di espandersi globalmente con facilità. Con i servizi basati sul cloud, le organizzazioni possono distribuire applicazioni e servizi a livello globale, servendo clienti in diverse sedi con la stessa forza lavoro che aveva già a disposizione. Questa accessibilità globale favorisce la collaborazione internazionale, accelera la penetrazione del mercato e permette interazioni fluide e senza interruzioni con un pubblico globale, superando le barriere geografiche.

L'evoluzione del cloud computing è appena agli inizi e nei prossimi anni i suoi impatti sulla tecnologia saranno ancora più profondi ¹⁹⁸, così com'è dimostrato all'articolo di Big Data 4 Innovation, nel 2023, le imprese continueranno a utilizzare i servizi cloud per accedere a tecnologie avanzate e migliorare l'efficienza delle loro operazioni. Si prevede che alcune delle tendenze principali includeranno un aumento degli investimenti nella sicurezza e nella resilienza del cloud, l'adozione di strategie multi-cloud, l'innovazione continua nell'ambito del cloud supportato dall'intelligenza artificiale, la crescita delle soluzioni per servizi low-code e no-code e il consolidamento nel settore del cloud gaming.

Se consideriamo il pesante impatto ambientale dei tradizionali data center, caratterizzati da un elevato consumo energetico e una grande impronta di carbonio, emerge la necessità di un'alternativa più sostenibile. Il cloud computing, con la sua infrastruttura condivisa e l'ottimizzazione delle risorse, offre proprio questa soluzione. I fornitori di servizi cloud migliorano l'efficienza energetica e riducono le emissioni di carbonio attraverso l'ottimizzazione delle operazioni dei data center. Inoltre, il modello pay-per-use minimizza lo spreco di risorse, contribuendo così agli obiettivi di sostenibilità e alla riduzione complessiva del consumo energetico.

Inoltre, ciò che si è voluto risaltare all'interno del lavoro di tesi è il tema della tutela del cliente andando ad analizzare dei contratti specifici di cloud (AWS e SAP). Esaminare le clausole specifiche di un contratto cloud, come quello previsto per l'implementazione di SAP in cloud o quello di AWS, offre un riscontro concreto su elementi cruciali che un'azienda deve valutare attentamente. Il confronto tra SAP e AWS evidenzia come i due fornitori adottino approcci differenti nei contratti cloud. AWS offre maggiore flessibilità e standardizzazione, mentre SAP tende a personalizzare i contratti in base alle esigenze specifiche dei clienti aziendali. Entrambi pongono grande enfasi su sicurezza, conformità e supporto tecnico, ma le modalità di implementazione e gestione variano significativamente, generando diversi impatti sull'azienda cliente. Di conseguenza, è fondamentale che le aziende valutino attentamente i termini contrattuali, le garanzie offerte e i potenziali rischi, adottando misure appropriate per mitigare questi ultimi e assicurare un'implementazione efficace e sicura del sistema cloud.

¹⁹⁸<https://www.bigdata4innovation.it/big-data/cloud-computing-cose-principali-tendenze-nel-2023/>

Tuttavia, nonostante i passi in avanti fatta dalla legislazione, è essenziale garantire una normativa più rigorosa per la tutela del cliente e la limitazione del potere del fornitore. Questa necessità emerge dalle numerose controversie tra le aziende e i fornitori di servizi cloud, causate da interruzioni dei servizi e da una deresponsabilizzazione dei fornitori. Oltre alla controversia tra BA e la CBRE, ce ne sono state molte altre, anche più recenti, che contribuiscono a sottolineare il necessario intervento normativo su questo settore.

In Europa, da qualche anno, si stanno già studiando misure per tutelare i clienti dei fornitori di servizi cloud, soprattutto con l'introduzione di regolamenti specifici, come ad esempio il GDPR (Regolamento Generale sulla Protezione dei Dati), che prevede norme rigide per la gestione dei dati personali, inclusi quelli nel cloud.

Inoltre, l'adozione di uno schema europeo di certificazione per i Cloud Service Provider potrebbe rappresentare un importante passo avanti per il rafforzamento del mercato interno dei servizi digitali. L'EUCS (European Union Cloud Service) è una certificazione che attesta la conformità dei fornitori di servizi cloud alle normative europee, e per ottenerla, i provider devono dimostrare di rispettare requisiti di sicurezza e privacy ¹⁹⁹.

Quindi, l'Europa si sta impegnando per garantire la protezione dei dati dei clienti e il rispetto delle normative da parte dei fornitori di servizi cloud, ma è fondamentale che le aziende valutino attentamente i fornitori e adottino misure di sicurezza efficaci.

In conclusione, è necessario ribadire che il cloud computing è il fulcro dell'evoluzione tecnologica, offrendo agilità, scalabilità e innovazione senza precedenti, ma è importante mantenere un equilibrio tra l'innovazione tecnologica e la tutela legale.

¹⁹⁹ <https://www.zerounoweb.it/cloud-computing/la-certificazione-europea-del-cloud-service-provider-cosa-e-importante-sapere/>

Bibliografia

Belisario, E. (2011). "Cloud Computing". Informatica Giuridica – collana diretta da Michele Iaselli - eBook n.17, Altalex.

Cardarelli, F. (1993). La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing, in dir. Informaz. Informatica.

Campagnoli MN., “Il cloud computing: vantaggi e problematicità”, pag 120.

Colangelo, G. (2012). L’enforcement del diritto d’autore nei Servizi Cloud. Dir. aut. II, 174.

Faggioli, G., & Italiano, A. (2017). I contratti di cloud computing. Comprendere affrontare e negoziare i contratti con i cloud provider. Franco Angeli.

Farina, M. (2018). I contratti informatici. Editore Key.

Iaselli, M. (2019). Lezioni di informativa giuridica. Key Editore.

Limone, M. (2018). Cloud computing. Aspetti contrattuali risvolti normativi e tutela della privacy. [Youcanprint](#), pp.58-59.

Mantelero, A. (2010). Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali, in Dir. informaz. informat., 673.

Mantelero, A. (2012). Il contratto per l’erogazione alle imprese di servizi di cloud computing. Contr. impr., IV-V, 1216.

Prandelli, E., & Verona, G. (2011). Vantaggio competitivo in rete dal web 2.0 al cloud computing.

Sartori, L. (2006). *Il Divario digitale. Internet e le nuove disuguaglianze sociali*. Il Mulino.

Troiano, G. (2011). *Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale: alla ricerca di un equilibrio tra diritti dell'utente e doveri del fornitore*. Cyberspazio e diritto.

Articoli & Documenti

Branshaw, S., Millard, C., & Walden, I. (2014). Standard contracts for cloud services. in C. Millard (Ed.), *Cloud Computing Law*. Oxford, pp. 44-46.

Campagnoli, M.N. (2018). Buone e/o cattive ragioni del cloud. Considerazioni alla luce del General Data Protection Regulation (GDPR). *Rivista giuridica on-line, ISSiRFA CNR*, pp. 5-8.

Garante per la protezione dei dati. “Cloud computing: indicazioni per l’utilizzo consapevole dei servizi”, pag. 9 e ss, <https://www.garanteprivacy.it/documents/10160/10704/1819933>.

Gallo, P. (2007). Asimmetrie informative e doveri di informazione, in “*Rivista di diritto civile*”.

Barki, H., Rivard, S., & Talbot, J. *Toward an Assessment of Software Development Risk*.

Lezioni di organizzazione dei sistemi informativi dell’azienda del Professore Francesconi e di metodologie e tecniche dell’impresa digitale del Professore Del Vecchio.

Camera di commercio industria artigianato e agricoltura di Torino. *La manutenzione del software: clausole commentate*, pp.8-9.

United Nations Commission on International Trade Law. (2019). *Notes on the Main Issues of Cloud Computing Contracts*.

Bellman, R. E., Clark, C. E., Craft, C. J., Malcolm, D. G., & Ricciardi, F. M. (1957). *On the Construction of a Multi-Stage Multi-Person Business Game*. RAND Corporation.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). *A Break in the*

Sitografia

<https://bsolutionsgroup.it/2019/08/29/da-capex-a-opex-il-cloud-e-la-sua-evoluzione-al-servizio-del-business/#:~:text=Quando%20la%20crisi%20economica%20del,quindi%20le%20risorse%20a%20budget>

<https://www.mdmtecnodocs.com/2021/11/il-cloud-al-tempo-del-covid-19/>

<https://www.smceconsulting.it/la-trasformazione-digitale-al-tempo-della-pandemia/>

<https://www.semplesio.it/ecommerce-in-cloud-a-cosa-serve-e-quali-sono-i-vantaggi/>

[Nel terzo trimestre 2021 il commercio digitale in Italia è cresciuto del 15% e si prevede ancora un Natale da record per l'e-commerce, ma attenzione all'aumento dei prezzi - Salesforce](#)

[Lambert Consulting - Statistiche e tendenze in Cloud Computing 2023 - 2024](#)

<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>

<https://aws.amazon.com/it/what-is-cloud-computing/>

<https://cloud.google.com/learn/what-is-cloud-computing?hl=it#:~:text=Cloud%20Computing%20Foundations-,Definizione%20di%20cloud%20computing,come%20i%20servizi%20su%20Internet>

<https://www.guru99.com/characteristics-of-cloud-computing.html#multitenancy-and-resource-pooling>

<https://www.atlassian.com/it/microservices/cloud-computing>

https://www.ctmobi.it/cloud/cloud-computing-cose-come-funziona-e-perche-conviene/#Le_cinque_caratteristiche_essenziali_del_Cloud_Computing

<https://vitolavecchia.altervista.org/definizione-caratteristiche-principali-del-cloud-computing/>

<https://www.ibm.com/it-it/topics/multi-tenant>

<https://www.securityopenlab.it/news/2254/le-5-best-practice-per-gestire-al-meglio-le-patch-di-sicurezza-dei-workload-cloud.html>

<https://cloud.google.com/learn/paas-vs-iaas-vs-saas?hl=it>

<https://www.redhat.com/it/topics/cloud-computing/iaas-vs-paas-vs-saas>

<https://injenia.it/inthinking/iaas-paas-saas-quali-differenze/>

<https://www.ibm.com/it-it/topics/iaas-paas-saas>

[Cos'è il modello IaaS? Infrastructure as a Service, Infrastruttura distribuita come servizio | Microsoft Azure](#)

[Cos'è una soluzione IaaS \(Infrastructure-as-a-Service\)? | IBM](#)

[https://www.ibm.com/it-it/topics/cloud-computing#:~:text=Il%20cloud%20computing%20%C3%A8%20un,servizi%20cloud%20\(o%20CSP\)](https://www.ibm.com/it-it/topics/cloud-computing#:~:text=Il%20cloud%20computing%20%C3%A8%20un,servizi%20cloud%20(o%20CSP))

<https://nds.id/en/public-cloud-en/>

[Che cos'è un cloud pubblico - Definizione | Microsoft Azure](#)

<https://www.redhat.com/it/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud>

<https://www.ibm.com/it-it/topics/public-cloud>

<https://www.gartner.com/en/newsroom/press-releases/2023-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023>

[Cos'è il cloud computing? | IBM](#)

[Che cos'è un cloud privato - Definizione | Microsoft Azure](#)

<https://www.spiceworks.com/tech/cloud/articles/what-is-community-cloud/>

[Rapporto sul mercato del cloud comunitario | Analisi e previsioni - 2032 \(alliedmarketresearch.com\)](#)

[Community Cloud Market Report | Analysis & Forecast - 2032 \(alliedmarketresearch.com\)](#)

[Cos'è il cloud ibrido e qual è il significato di ambiente cloud? | Cloudflare](#)

[Che cos'è il cloud ibrido? - Vantaggi e svantaggi di un cloud ibrido | NetApp](#)

[Cloud Ibrido: cosa è ed i vantaggi - IWS Consulting](#)

<https://www.mordorintelligence.com/industry-reports/hybrid-cloud-market>

[Mercato Cloud Computing in Italia in crescita del 19% \(osservatori.net\)](#)

<https://www.lambertconsulting.ch/it/statistiques-et-tendances-du-cloud-computing-2023-2024/>

<https://www.vmware.com/it/topics/glossary/content/multi-cloud-strategy.html>

<https://cloud.google.com/learn/what-is-hybrid-cloud?hl=it>

<https://www.akamai.com/it/glossary/what-is-hybrid-cloud>

<https://cloud.google.com/learn/advantages-of-cloud-computing?hl=it>

<https://www.cybersecurity360.it/legal/privacy-dati-personali/servizi-cloud-e-compliance-gdpr-obblighi-e-soluzioni/>

<https://cloud.google.com/learn/what-is-cloud-data-security?hl=it>

<https://www.aruba.it/magazine/cloud/lock-in-come-evitarlo-e-come-uscirne-con-successo.aspx>

<https://magazine.wiit.cloud/cloud-as-a-service-le-4-criticita-pi%C3%A0-sottovalutate-e-come-risolverle>

https://docs.italia.it/italia/cloud-italia/strategia-cloud-italia-docs/it/stabile/2_il_cloud_computing.html

<https://www.ht-avvocati.it/obbligazioni-debiti-crediti/debiti-crediti-tipi-obbligazione/obbligazione-mezzi-risultato.php>

<https://www.riskmanagement360.it/analisti-ed-esperti/software-le-varie-tipologie-di-contratti/>

<https://assets.kpmg.com/content/dam/kpmg/it/pdf/2018/02/Hybrid-IT-at-scale.pdf>

<https://softwarebusiness.it/la-matrice-raci-nella-definizione-di-ruoli-e-responsabilita-nel-sistema-sap/>

<https://www.entersoftware.it/kpi-aziendali/>

<https://www.egovaleo.it/geek-lab/business-analyst-cosa-fa-e-competenze/><https://www.egovaleo.it/geek-lab/business-analyst-cosa-fa-e-competenze/>

<https://vitolavecchia.altervista.org/professione-informatica-la-figura-del-business-analyst/>

<https://www.bucap.it/news/appfondimenti-tematici/continuta-operativa/cloud-caratteristiche.htm>

<https://www.altalex.com/documents/news/2021/11/23/contratto-cloud-raggi-x>

https://www.edpb.europa.eu/news/news/2021/edpb-adopts-opinions-first-transnational-codes-conduct-statement-data-governance-act_it

<https://en.iusintech.com/il-contratto-di-cloud-computing/>

<https://www.zerounoweb.it/cloud-computing/contratti-cloud-le-clausole-da-tenere-d-occhio/#:~:text=In>

<https://www.agendadigitale.eu/sicurezza/contratto-cloud-computing-la-guida-completa-ecco-come-funziona/>

<https://www.keliweb.it/tos.php>

<https://avvocato360.it/news/diritto-di-recesso-quando-si-puo-esercitare>

<https://www.digital4.biz/executive/guida-alla-scelta-del-cloud-provider-aspetti-da-valutare/>

<https://www.vincenzocalabro.it/article/2024/minacce-e-vulnerabilita-del-cloud-computing-come-proteggersi.html>

<https://www.agendadigitale.eu/cultura-digitale/aria-agcom-la-complessa-mission-dellautorita-nellattuale-mosaico-digitale/>

https://it.wikipedia.org/wiki/British_Airways

[CBRE nominata per la gestione del patrimonio globale di British Airways \(europe-re.com\)](https://www.europe-re.com/it/2024/03/20/cbre-nominata-per-la-gestione-del-patrimonio-globale-di-british-airways/)

https://www.linkedin.com/pulse/cloud-skies-scope-computing-aviation-industry-rajat-nayar?trk=portfolio_article-card_title

<https://www.aviationfile.com/cloud-computing-in-aviation/>

<https://www.nutanix.com/it/info/what-is-hybrid-cloud>

<https://www.forbes.com/sites/forbestechcouncil/2022/03/03/how-cloud-technology-can-enhance-your-airport-experience/>

<https://www.ibm.com/it-it/topics/cloud-computing-benefits>

[British Airways private cloud takes flight with Juniper Networks | ITPro](https://www.itpro.it/2024/03/20/british-airways-private-cloud-takes-flight-with-juniper-networks/)

<https://www.cbre.co.uk/services/industries/aviation>

<https://www.appvizer.it/rivista/organizzazione/facility/facility-management>

https://it.wikipedia.org/wiki/Cloud_computing

[cbre-supplier-code-of-conduct-italian.pdf](https://www.cbre.com/~/media/Files/2024/03/20/cbre-supplier-code-of-conduct-italian.pdf)

<https://europe-re.com/cbre-appointed-to-manage-british-airways-global-estate/24658>

<https://www.datacenterknowledge.com/uptime/cbre-settles-british-airways-lawsuit-over-costly-data-center-outage>

<https://www.computerweekly.com/news/252457343/British-Airways-settles-legal-claim-with-CBRE-over-May-2017-Bank-Holiday-datacentre-outage>

<https://www.zerounoweb.it/cloud-computing/la-certificazione-europea-del-cloud-service-provider-cosa-e-importante-sapere/>