Università
Ca'Foscari
Venezia

Corso di Laurea magistrale
in Economia e Gestione delle Aziende

Ca' Foscari
Dorsoduro 3246
30123 Venezia

Tesi di Laurea

GLI ASPETTI DELLA SICUREZZA NEI CONTRATTI DI CLOUD COMPUTING

Relatore
Ch. Prof. Giovanni Vaia

Laureando
Matteo Pace
Matricola 810970

Anno Accademico
2012 / 2013

Indice

Introduzione **6**

Capitolo 1 LE BASI DEL CLOUD COMPUTING **9**

1.1 Introduzione al concetto di cloud computing..... 9

1.2 Gli albori del cloud computing..... 10

1.3 Le caratteristiche principali del SOA..... 11

1.4 Il concetto alla base del funzionamento del cloud computing:

la virtualizzazione dei server..... 14

1.5 I tre tipi di servizi offerti dal cloud computing..... 16

1.5.1 Software as a service..... 16

1.5.2 Platform as a service..... 18

1.5.3 Infrastructure as a service..... 20

1.6 I diversi modelli di sviluppo di una piattaforma cloud..... 23

1.6.1 Public cloud..... 23

1.6.2 Private cloud..... 25

1.6.3 Community cloud..... 26

1.6.4 Hybrid cloud..... 27

1.7 Quale cloud é la scelta migliore per l'impresa?..... 28

1.8 La private cloud é davvero l'opzione più adatta per la sicurezza dell'azienda?..... 29

1.9 La diffusione capillare e le prospettive future..... 31

1.9.1 Gli incentivi offerti dall'Europa alla crescita del cloud computing..... 32

1.9.2 Anche le organizzazioni governative optano per l'uso di piattaforme cloud..... 35

1.9.3 Il cloud computing nei Paesi in via di sviluppo..... 36

1.9.4 I dati attuali e l'evoluzione prospettica..... 40

Capitolo 2 BENEFICI E RISCHI LEGATI AL CLOUD COMPUTING 42

2.1 Gli elementi principali che spingono le aziende ad affidarsi al cloud computing..... 42

2.2 I rischi correlati all'uso di piattaforme cloud e come agire per fronteggiarli..... 52

2.3 I costi del cloud computing..... 57

2.4 I fattori che portano l'azienda a sviluppare un modello cloud ottimale..... 59

Capitolo 3 LA SCELTA DEL CLOUD COMPUTING E I CORRISPETTIVI RISVOLTI AZIENDALI 62

3.1 Aspetti da considerare prima di avventurarsi nel cloud..... 62

3.2 Il cloud adoption lifecycle..... 68

3.2.1 La fase della scelta del tipo di strategia da adottare..... 69

3.2.2 La fase della scelta del provider e del tipo di cloud..... 71

3.2.3 La fase del testing..... 71

3.2.4 La fase dell'azione concreta..... 72

3.3 L'incidenza sulle risorse umane..... 73

3.4 Alcuni esempi pratici di adozione di piattaforme cloud..... 74

Capitolo 4 IL CONTRATTO TRA PROVIDER E CLIENTE E LA PROBLEMATICA DELLA SICUREZZA 78

4.1 La stipula del contratto..... 78

4.2 Gli elementi che impattano sulla sicurezza nei contratti cloud..... 97

4.2.1 Akamai..... 100

4.2.2 Amazon..... 103

4.2.3 Apple..... 107

4.2.4 Dropbox..... 110

4.2.5 Facebook..... 114

4.2.6 Google..... 117

4.2.7 IBM..... 121

4.2.8 Microsoft..... 124

4.2.9 Rackspace..... 128

4.2.10 Salesforce.com..... 131

4.2.11 Rappresentazione sommaria dei risultati ottenuti..... 135

4.3 Le minacce alla sicurezza dei dati e le misure per contrastarle..... 137

4.3.1 Gli attacchi DDoS..... 137

4.3.2 L'encryption dei dati..... 140

Conclusioni **141**

Bibliografia **144**

Introduzione

La crescita del cloud computing, lo dicono in modo esplicito le statistiche che si occupano di rilevarne la propagazione, é continua e vertiginosa; la possibilità di avere accesso a servizi IT, senza doversi dotare internamente delle strutture richieste per il loro funzionamento, ma semplicemente pagando un servizio ad un provider esterno, é uno scenario troppo "ghiotto" per non essere sfruttato dalle singole imprese presenti nel mercato attuale.

Se, inizialmente, affidarsi a servizi cloud significava intraprendere una vera e propria svolta all'interno della strategia operativa aziendale, oggi, tale approccio costituisce una "*conditio sine qua non*" per le start-up e le aziende medio-piccole e una discriminante non banale per quelle di più elevata dimensione, per "destreggiarsi" al meglio all'interno dei "meandri" del contesto competitivo di riferimento. Come vedremo più approfonditamente in seguito, il risparmio in termini di denaro, tempo e risorse, solitamente dedicato alle componenti IT, ottenibile grazie al cloud computing, rappresenta una variabile strategica importante per le imprese, nonché, al giorno d'oggi, spesso, un requisito base per poter "battagliare ad armi pari" con la concorrenza.

In un contesto del genere, in cui si condivide con un soggetto esterno la gestione di un determinato ammontare di dati sensibili, la componente della sicurezza all'interno dei contratti tra provider e cliente assume carattere prioritario; i "T&C" (Terms & Conditions) contrattuali elencati dal provider per l'utilizzo dei suoi servizi dovrebbero, infatti, rivelarsi il più possibile idonei a tutelare il cliente.
Compito principale di questa tesi, sarà proprio verificare il grado di tutela tendenzialmente offerto ad un cliente generico che si affida a soluzioni cloud.

Nel primo capitolo inizieremo ad addentrarci all'interno del "mondo cloud" cominciando dalla definizione, le origini e i concetti base, fino a riscontrarne il grado di diffusione attuale e l'evoluzione prospettica.

Il secondo capitolo si occuperà di illustrare i benefici e i rischi del cloud computing indicando, a conclusione della discussione, i fattori che portano a sviluppare un modello cloud ottimale.

Nel terzo capitolo si passerà direttamente agli aspetti pratici; verranno considerati gli elementi fondamentali legati alla scelta del cloud computing, le fasi da seguire per arrivare al suo effettivo utilizzo e alcuni esempi pratici attuali riguardanti la sua adozione.

Infine, all'interno del quarto e ultimo capitolo si affronterà, nel dettaglio, il momento della stipula del contratto per la fruizione dei servizi cloud, seguito da un confronto delle peculiarità dei "T&C" offerti da 10 dei più rinomati provider a livello internazionale. Poi, sfruttando i dati raccolti, ci si focalizzerà scrupolosamente sugli elementi che impattano sulla sicurezza del cliente; nello specifico, verrà fatta un'analisi, provider per provider, in termini di "*confidentiality*", "*integrity*" e "*availability*" assicurate nella gestione dei dati del cliente e, dai risultati ottenuti, ne scaturirà un quadro specifico caratterizzante la tendenza in atto, in termini di sicurezza nei contratti, all'interno dell'intero universo del cloud computing.

Capitolo 1

LE BASI DEL CLOUD COMPUTING

1.1 Introduzione al concetto di cloud computing

Quando ci si riferisce al termine “cloud computing”, in linea generale, si indicano quei prodotti, servizi e soluzioni, per il singolo consumatore e per le aziende, che vengono distribuiti e utilizzati, in tempo reale e su esplicità domanda, tramite internet.

La più adottata, completa e dettagliata definizione é, però, senza dubbio quella fornita dal NIST[1] che definisce il “cloud computing” come “*un modello che permette l'accesso ad un condiviso insieme di risorse informatiche configurabili (come, ad esempio, network, server, piattaforme di immagazzinamento dati, applicazioni e altri*

1 Il NIST (National Insitute for Standards and Technologies) è un'agenzia del governo degli Stati Uniti d'America che si occupa della gestione delle tecnologie. Fa parte del Dipartimento del Commercio e il suo compito è la promozione dell'economia americana attraverso il lavoro con l'industria per sviluppare standard, tecnologie e metodologie che favoriscano la produzione e il commercio.

servizi) da ogni zona e con un cospicuo risparmio in termini di costo, usufruibile rapidamente e con un minimo intervento da parte del management e bassa necessità di intermediazione da parte del fornitore del servizio"[2].

Grazie all'avvento delle piattaforme cloud, infatti, i fruitori dei servizi da esse offerti possono beneficiare della possibilità di utilizzare risorse hardware e software, messe a disposizione da un terzo, in modo semplice, con un notevole risparmio in termini economici e senza la necessità di sapere esattamente dove i server, su cui si poggiano tali hardware e software, siano fisicamente collocati.

Questi aspetti, come vedremo in seguito più nel dettaglio, sono alla base della capillare diffusione e notevole crescita del "cloud computing" a livello globale, sia per quanto riguarda le piccole (le start-up ne sono una dimostrazione pratica) sia per ciò che concerne le medio/grandi imprese.

1.2 Gli albori del cloud computing

La crisi economica mondiale, iniziata nel 2008, nella molteplicità degli effetti causati, ha aumentato anche l'incertezza legata agli investimenti in IT.

La diretta conseguenza di questa situazione é stato il cambiamento di strategia della maggior parte delle imprese, che hanno abbandonato complesse iniziative di

2 Peter Mell, Tim Grance, *The NIST definition of cloud computing,* Communications of the ACM, 2010.

trasformazione come il "SOA[3]", a favore di servizi più concreti e con grande potenziale di immediato recupero dell'investimento iniziale, come il "cloud computing".

Questa transizione ha permesso alle aziende di trasferire il rischio (oltretutto se si verificheranno problemi ad un server, il "cloud provider" si occuperà immediatamente di risolverli, qualunque essi siano, avendo la capacità di riparare o rimpiazzare ciò che non funziona quasi istantaneamente, a differenza del tempo, quantificabile in settimane o mesi, necessario, spesso, per ovviare ad un problema legato ad un server interno all'azienda) e il costo legato agli investimenti tecnologici in data center e applicazioni software, a fornitori esterni altamente specializzati in tale ambito.

1.3 Le caratteristiche principali del SOA

L'avvento del SOA (Service Oriented Architecture) ha accelerato lo sviluppo dei componenti software che sono alla base del cloud computing.

Quando si parla di SOA ci si riferisce, semplicisticamente, ad un'architettura software che suddivide i vari dati a disposizione dell'azienda in codici.

3 "*SOA*": nell'ambito dell'informatica, con la locuzione inglese di **Service-Oriented Architecture** (SOA) si indica generalmente un'architettura software adatta a supportare l'uso di servizi web per garantire l'interoperabilità tra diversi sistemi, così da consentire l'utilizzo delle singole applicazioni come componenti del processo di business e soddisfare le richieste degli utenti in modo integrato e trasparente. (Wikipedia)

Così facendo, nel momento in cui qualsiasi soggetto all'interno dell'impresa necessiti di dover consultare uno specifico campione di dati all'interno del database, gli sarà sufficiente conoscere il codice corrispondente per averne un immediato accesso.

Questo porta ad un notevole risparmio di tempo a disposizione dei dipendenti (utilizzabile per altri fini aziendali) e consente di diffondere chiarezza su come l'azienda organizza le proprie applicazioni e l'architettura software di base.

SOA, inoltre, agli occhi dei manager é un approccio molto attrattivo, in quanto aiuta questi ultimi ad effettuare veloci cambiamenti alle applicazioni esistenti, o a crearne di nuove, in risposta all'evoluzione del mercato e/o al manifestarsi di diverse esigenze di business.

Tutti questi motivi fanno si che un'impresa che abbia deciso di affidarsi al SOA, affronti l'evoluzione verso il cloud computing in modo lineare, immediato e quasi naturale. Le piattaforme cloud, infatti, si poggiano sui precetti e gli elementi caratteristici dell'infrastruttura tipica della “service oriented architecture”, ragion per cui un'organizzazione che ha precedentemente usufruito del SOA con successo, é meglio posizionata di qualunque altra per primeggiare in seguito all'adozione del cloud computing.

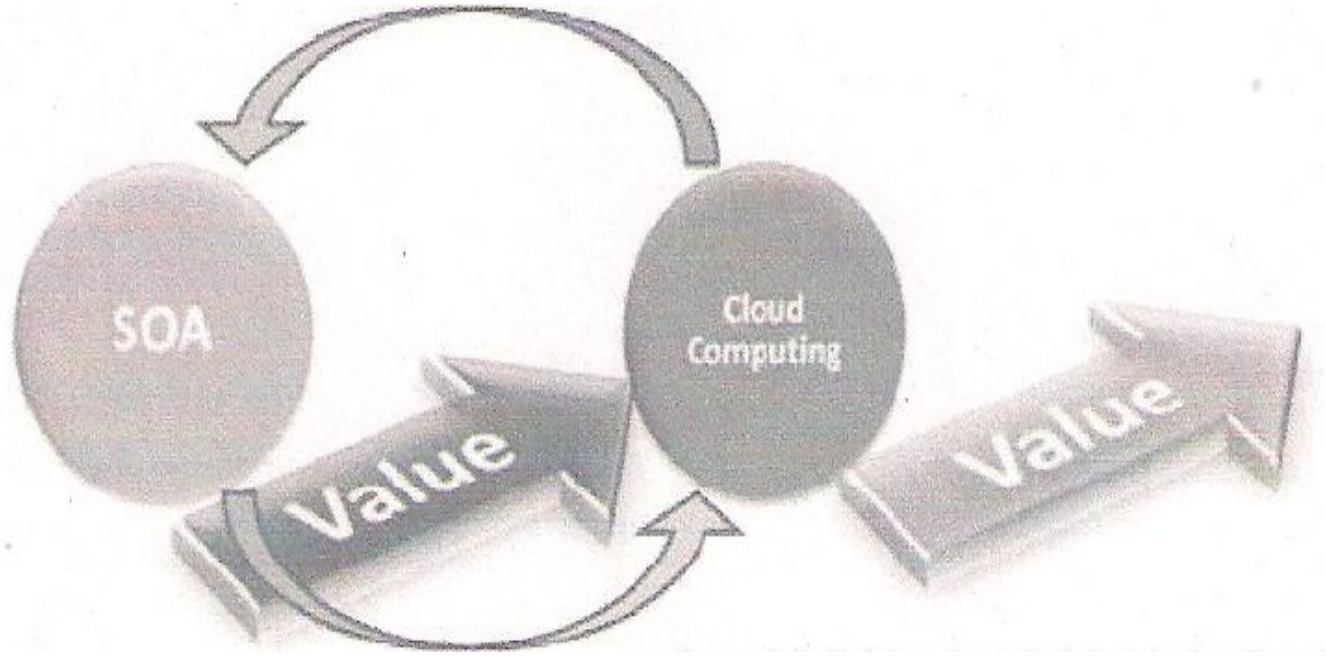

Figura 1.1: Il valore aziendale creato dall'interazione SOA-Cloud Computing (Eric A. Marks e Bob Lozano, *Executive's guide to cloud computing*, Wiley, Hoboken, 2010)

Occorre specificare che quest'ultimo ragionamento é valido in caso di imprese di grandi dimensioni, che necessitano di un'architettura software tanto dettagliata quanto complicata da realizzare.

Se, invece, prendiamo in considerazione aziende medio-piccole, o vere e proprie start-up, la dotazione di un modello SOA risulta ad esse poco utile e, in generale, sconveniente; in questo caso, infatti, la semplicità della struttura e la possibilità di controllare agevolmente la mole di dati a disposizione, consiglia un'adozione diretta di piattaforme cloud.

1.4 Il concetto alla base del funzionamento del cloud computing: la virtualizzazione dei server

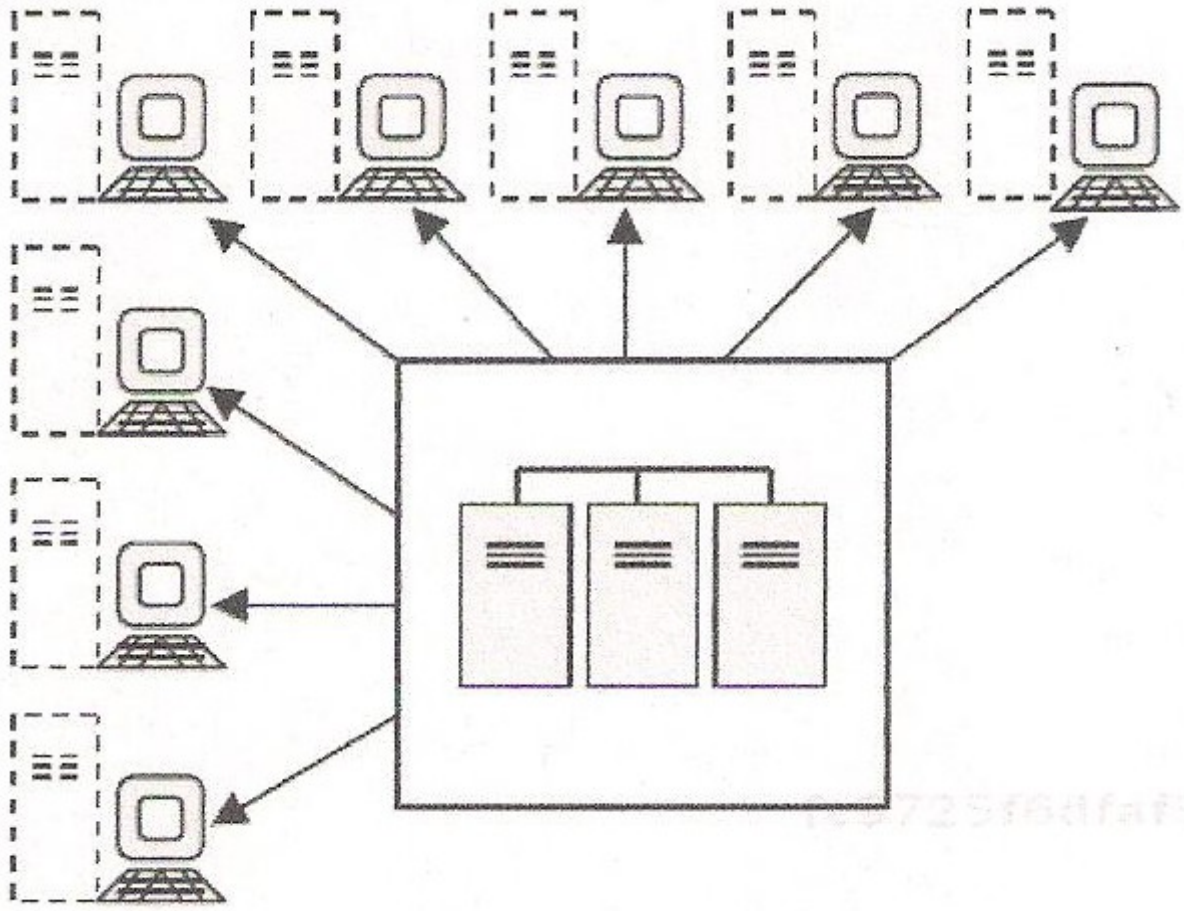

Figura 1.2: Server virtualization (Michael H. Hugos, Derek Hulitzky, *Business in the cloud: what every business needs to know about cloud computing*, Wiley, Hoboken, 2010)

La "virtualizzazione dei server" é il meccanismo fondamentale che costituisce la base del funzionamento del cloud computing.

Quando si parla di virtualizzazione, si fa riferimento al processo di creazione di una copia in software di un elemento all'interno del contesto costituito dal "computing"

(nel nostro caso, un server). All'utilizzatore del server sembrerà di avere tutte le risorse di quest'ultimo a propria completa disposizione, ma la realtà é un'altra; il server offre solo una parte della sua totale capacità operativa a supporto dell'utente in questione, mentre la parte restante é suddivisa tra molti altri utenti, tutti alle prese con la propria copia virtuale del server considerato.

Questo consente di sfruttare adeguatamente l'intero potenziale del server stesso che all'interno delle aziende é quasi sempre sottoutilizzato (andando a rappresentare, così, un notevole spreco di denaro). Le conseguenze dirette di tale modello sono, quindi, un notevole risparmio monetario per il consumatore, ma anche per il fornitore del servizio che, grazie alle caratteristiche della virtualizzazione dei server, riesce a raggiungere rilevanti economie di scala.

1.5 I tre tipi di servizi offerti dal cloud computing

1.5.1 Software as a service

Il primo, e probabilmente più conosciuto, dei servizi offerti dalle piattaforme cloud é il “SaaS” (Software as a service).

Tramite esso, il fornitore del servizio mette a disposizione un'applicazione senza che il cliente, utilizzandola, sia costretto ad esserne il proprietario, a doverla installare su ogni singolo computer che ne deve fare uso, ad occuparsi dei relativi aggiornamenti e delle installazioni di “patch” a scopo protettivo e a doverla mantenere all'interno del suo “data center”[4]; questi oneri, infatti, spettano al “cloud provider” (il fornitore del servizio che si basa sulla tecnologia cloud).

Il cliente, quindi, può beneficiare del servizio offerto da qualsiasi luogo, semplicemente utilizzando un dispositivo tramite cui é possibile connettersi alla rete internet.

Ciò detto, non va dimenticato che i servizi SaaS sono parecchio ambiti anche per un altro importante fattore; essi, infatti, grazie alla possibilità di trasferire le procedure di acquisto, installazione e manutenzione ad un fornitore esterno, permettono di eliminare il bisogno di rilevanti investimenti interni in conoscenza e preparazione informatica, consentendo, così, un deciso risparmio in termini di tempo e denaro.

4 “Centro elaborazione dati”; è l'unità organizzativa che coordina e mantiene le apparecchiature ed i servizi di gestione dei dati.

Analizziamo, ora, i diversi casi in cui é conveniente, per l'azienda, rivolgersi a questo tipo di servizi e quelli in cui, invece, essi non risultano essere la soluzione più adatta.

Situazioni in cui conviene utilizzare servizi SaaS:

- Il software da adottare rappresenta un tipo di tecnologia fondamentale per fare business, ma risulta anche essere il medesimo per tutti gli attori in gioco (dal suo utilizzo non scaturisce, cioé, alcun vantaggio competitivo).

  Un esempio di questo tipo di situazione, può essere rappresentato dall'e-mail aziendale.

- Applicazioni in cui c'é un continuo interscambio di informazioni tra l'organizzazione e il mondo esterno, come nel caso di software adibiti all'invio di “newsletter” informative a clienti effettivi e potenziali.

- Software di cui si ha bisogno solo per un breve termine (e che, quindi, non conviene acquistare, ma “affittare”), come nel caso di un tipo di collaborazione tra più soggetti, destinata a terminare una volta raggiunto l'obiettivo alla base dell'esistenza della stessa.

- Software il cui utilizzo é altamente altalenante come, ad esempio, l'insieme delle applicazioni inerenti il sistema tributario (strettamente necessarie, ma di cui ci si serve raramente).

Situazioni in cui non conviene utilizzare servizi SaaS:

- Applicazioni nelle quali la legge o altri tipi di regolamentazioni non consentono di trasferire i dati all'esterno dell'organizzazione.

- Applicazioni in cui é richiesta un'analisi dettagliata ed estremamente veloce di dati in tempo reale.

Si ritiene, universalmente, che la prima società ad aver introdotto dei servizi di tipo SaaS sia stata “Salesforce.com”, attraverso un'applicazione finalizzata al “CRM” (Customer Relationship Management).
Dopo di essa, lo sviluppo di applicazioni di questo genere ha invaso anche altre aree, quali l'e-mail, i servizi finanziari, il monitoraggio delle spese aziendali e, negli ultimi anni, i “social network”.
“Gmail”, “Facebook”, “LinkedIn”, “YouTube”, “Google Docs”, “Office 365” e “Yahoo” sono solo alcuni tra i più noti esempi di servizi SaaS contemporanei, largamente utilizzati dagli utenti del “web”, che si basano sui precetti illustrati.

1.5.2 Platform as a service

Quando si parla di “PaaS” (Platform as a service) ci si riferisce ad una piattaforma software in cui il cliente può creare, sviluppare e testare applicazioni usufruendo degli strumenti forniti dal provider. (-Pat Helland, *“Condos and clouds”*,

Communications of the ACM, 2013-).

Questo tipo di servizio permette, dunque, all'utilizzatore di eliminare il bisogno di dover acquistare, sviluppare e mantenere strutture interne, adeguate alla creazione e all'utilizzo di applicazioni software.

Facendo un confronto diretto con le applicazioni SaaS, si può dire che i concetti siano analoghi, con la differenza che, nel caso SaaS si tratta di applicazioni software distribuite all'interno della rete internet, mentre nel caso PaaS si tratta di piattaforme a disposizione per la creazione di applicazioni software distribuite all'interno della rete internet.

Le piattaforme PaaS sono nel pieno di uno sviluppo sostanziale, in quanto sempre più ampiamente adottate da organizzazioni e sviluppatori di tutto il mondo; la loro tangibile caratteristica di giovarsi sia della semplicità dei servizi SaaS, sia del potere caratterizzante i servizi IaaS, le rende un'opzione sempre più appetibile per il vasto mondo degli utenti interessati.

Nello specifico, questo tipo di utenti sono rappresentati, generalmente, da un insieme di soggetti contemporaneamente coinvolti nello sviluppo di un determinato progetto aziendale; l'aspetto principale che rende questo tipo di servizi fondamentali dal punto di vista competitivo, é l'intenzione di usufruirne per automatizzare la fase di “testing” e procedere, quindi, al continuo miglioramento dei progetti aziendali stessi.

“Google App Engine”, “Force.com”, “Microsoft Azure Services”, “Appistry”, “3Tera”, “Rightscale”, “Enomaly”, “Eucalyptus”, “Cloudera”, “Gigaspaces” e “Terracotta”, giusto per fare alcuni esempi, sono popolari soluzioni PaaS

pubblicamente accessibili da chiunque sia dotato di un dispositivo con connessione internet.

1.5.3 Infrastructure as a service

Le piattaforme “IaaS” (Infrastructure as a service) permettono ai dipartimenti IT delle aziende di affittare una piattaforma hardware “virtuale” e, susseguentemente, configurare, on-line, il server e le applicazioni software di cui si necessita (godendo dello spazio di data center desiderato) usufruendo dell'equipaggiamento funzionale al tipico operare di un network aziendale; tutto questo avviene semplicemente “su domanda”, senza l'obbligo e la preoccupazione, quindi, di dover acquistare materialmente alcun componente hardware (si procede esclusivamente al pagamento del servizio nei termini in cui si intende beneficiarne). (-Dave Durkee, “*Why cloud computing will never be free*”, Communications of the ACM, 2010-)

Esistono alcuni casi in cui é strettamente consigliabile, per l'organizzazione, rivolgersi a questo tipo di servizi e altri, invece, in cui una scelta simile potrebbe risultare svantaggiosa.

Di seguito ne analizziamo i più importanti.

Situazioni in cui conviene utilizzare servizi IaaS:

- Quando l'organizzazione sta crescendo rapidamente e avere a disposizione un hardware interno della capacità adeguata ai servizi continuamente richiesti, potrebbe risultare problematico (problemi di scalabilità).

- In caso di nuove organizzazioni non dotate di capitale sufficiente da investire in risorse hardware (un tipico esempio sono le start-up).

- Quando la domanda dei consumatori é parecchio volatile e dotarsi di un'infrastruttura IT di dimensione adatta ai continui cambiamenti dei flussi, diventa complicato.

- Quando all'interno dell'organizzazione ci sono pressioni per una limitazione e, possibilmente, riduzione delle spese in conto capitale a favore di quelle di tipo operativo.

- In caso di specifiche linee di business, progetti pilota o altri bisogni temporanei di strutture IT.

Situazioni in cui non conviene utilizzare servizi IaaS:

- Nel caso in cui alcune leggi o regolamenti risultino di ostacolo al trasferimento e immagazzinamento di dati dall'organizzazione ad un ente autonomo esterno ad essa.

- Quando sono richiesti i più alti standard di performance e le infrastrutture IT dedicate, di cui l'impresa si é dotata, rispondono già ai requisiti di cui essa ha bisogno.

In realtà, al giorno d'oggi, il confine tra piattaforme IaaS e PaaS sta divenendo sempre più labile: la fornitura di servizi IaaS collegati a strumenti che aiutino con la configurazione e permettano lo sviluppo di servizi di diverso genere non sono, infatti, più l'eccezione, ma la regola.

“Amazon Web Services”, “Rackspace”, “Savvis”, “HP”, “IBM” e “Dell” sono esempi di fornitori di servizi di questo genere, disponibili su richiesta del cliente.

1.6 I diversi modelli di sviluppo di una piattaforma cloud

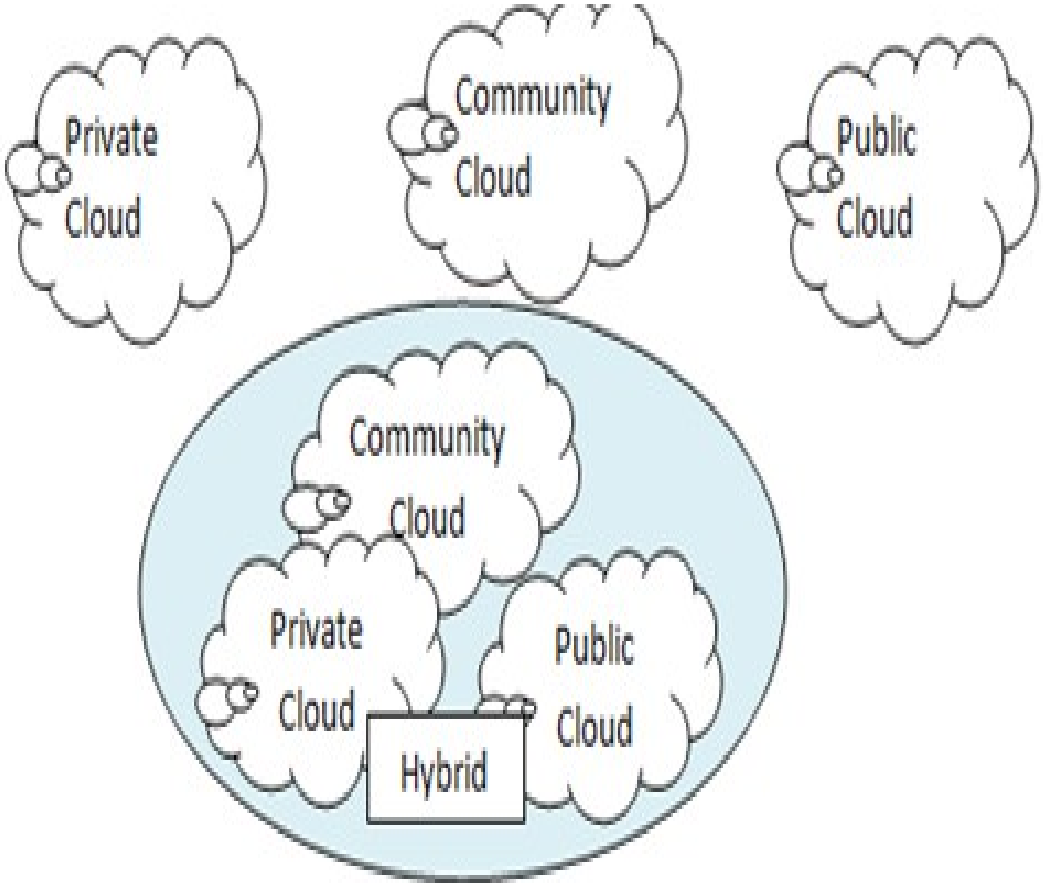

Figura 1.3: Cloud Deployment Options (http://www.eadynamicsuk.com/?name=pages&page=TOGAF__Cloud_Computing**)**

1.6.1 Public Cloud

La “public cloud” si caratterizza, tipicamente, per il suo approccio “multi-tenancy”; generalmente, infatti, consente l'utilizzo della sua infrastruttura, e dei servizi ad essa collegati, a più clienti provenienti da diverse organizzazioni.

Per ottenere un profitto, naturalmente, il fornitore del servizio impone un limite fisico, per ciascun beneficiario, all'ammontare di risorse condivise disponibili all'interno della propria piattaforma cloud. Limite che é superabile solo nel caso in cui, nel “service level agreement” iniziale (contratto stipulato inizialmente tra le parti in gioco), il cliente si sia accordato con il “provider” per un supplemento, dietro pagamento di un “premio” (un'ulteriore quota di denaro).
L'accordo iniziale, però, non permette al cliente di specificare esplicitamente come verranno forniti i servizi di “cloud computing” e, quindi, il controllo sostanziale delle operazioni rimane in mano al “provider”. Tale assunto insinua, però, il dubbio che, qualcuno di coloro i quali lavorano per l'offerta dei servizi di risorse condivise, possa avere accesso ai dati dei clienti senza il permesso di quest'ultimi. Questo potenziale problema legato alla sicurezza é, di conseguenza, il motivo per cui molti potenziali adottatori dei servizi cloud si orientano verso l'adozione di una “private cloud”.

Ciò nonostante, però, esistono svariati motivi per i quali un'organizzazione dovrebbe scegliere di affidarsi al cloud computing adottando una “public cloud”:

- *Basso costo: s*i tratta, infatti, del tipo di cloud che richiede il più basso investimento per l'utilizzo, prestandosi, così, ad esempio, come ottima soluzione per il “testing” di progetti aziendali in fase embrionale e/o dall'esito incerto.

- *Basso rischio:* come detto, con questo tipo di “nuvola”, l'organizzazione può sperimentare velocemente soluzioni legate al cloud computing dovendo tollerare un rischio minimo.

- *Paghi solo per ciò che ti serve/utilizzi:* le public cloud si basano su un modello di costo variabile. Questo permette all'azienda, una volta completato il progetto, o nel caso in cui non si abbia più bisogno dei servizi cloud offerti, di terminare il pagamento annesso.

- *Rapido accumulo di conoscenza, abilità ed esperienza:* é, infatti, grande la possibilità, per lo staff aziendale, di sfruttare il lavoro del “provider” e acquisire velocemente nozioni e abilità riguardanti il mondo del cloud computing. Ciò permette di intuire come operare più efficacemente ed efficientemente all'interno di una strategia operativa improntata su meccanismi cloud e cercare di conseguire, quindi, un vantaggio competitivo sui concorrenti.

1.6.2 Private Cloud

La “private cloud”, come si intuisce dal nome, consente all'organizzazione, che decide di adottarla, di avere il controllo esclusivo sull'infrastruttura e i servizi che offre e di permettere l'accesso alle risorse condivise solo ai membri

dell'organizzazione stessa. Si é specificato “controllo”, in quanto l'azienda non é essa stessa creatrice dell'entità di servizi a cui ha accesso, ma, appunto, ne acquisisce l'utilizzo, (o il vero e proprio possesso), come unico attore, tramite un contratto con un “provider” esterno.

Questo particolare tipo di cloud consente, quindi, di ovviare alle preoccupazioni legate alla privacy e alla gestione sicura dei dati, che caratterizzano l'avvicinamento dei manager alla soluzione “public”.

1.6.3 Community Cloud

Una “community cloud” si può definire come un gruppo unito da una causa o scopo comune. Essa, infatti, viene creata appositamente (e, quindi, con caratteristiche peculiari che la differenziano da una cloud generica) per essere destinata ad uno specifico gruppo di utenti, che la sfruttano per condividere dati e coordinare le rispettive mansioni e gli specifici compiti a cui devono assolvere (la condivisione di costi e vantaggi dei servizi cloud tra più soggetti viene, nel linguaggio comune, definita “approccio multitenancy”).

Esempi concreti di fruitori di questo particolare tipo di “nuvola”, possono essere soggetti che instaurano collaborazioni nel campo dei servizi finanziari o della salute.

1.6.4 Hybrid Cloud

L' “hybrid cloud”, tipicamente, condivide aspetti di tutti e tre i modelli precedenti. Essa viene adottata da un numero sempre più crescente di utenti, per riuscire a combinare tra loro gli aspetti positivi delle altre cloud e poter, così, meglio integrare i propri servizi al suo interno.

Combinazione, però, che si preannuncia a dir poco complessa, in quanto la decisione di come distribuire le applicazioni in una struttura sia “private” che “public” può non essere affatto semplice. (-Kamal Srivastava, Atul Kumar, “*A new approach of cloud computing infrastructure on demand”*, Trends in information management, 2011-) Nonostante ciò, “molti ricercatori affermano che, in breve tempo, ci saranno solo hybrid cloud“[5] e, se così sarà, la loro diffusione sarà pressoché illimitata.

Per questo motivo, compagnie IT come Cisco, Itricity, Juniper Networks e Nimsoft, che si occupano della tecnologia necessaria per l'utilizzo di questo tipo di modello da parte delle imprese, prospettano già lauti guadagni futuri.

5 Eric A. Marks e Bob Lozano, *Executive's guide to cloud computing,* Wiley, Hoboken, 2010.

1.7 Quale cloud é la scelta migliore per l'impresa?

Se l'azienda presa in considerazione é una start-up, é sensato che essa usufruisca immediatamente di una “public cloud”, invece di investire preziose quantità di capitale nel dotarsi di propri “data center” (quantità di capitale di rilevanza tale che, spesso, risultano anche fuori portata).

Questa scelta, inoltre, permette all'organizzazione di poter concentrare tutte le proprie energie nello sviluppo del prodotto o servizio che sarà alla base dei profitti futuri, senza perderne alcuna nell'acquisto/sviluppo dei componenti hardware e software, di cui si avrà bisogno all'interno dei processi produttivi.

Nel caso, invece, di aziende già esistenti che hanno investito, negli anni, nella realizzazione e nel funzionamento di modelli operativi di software interni, é opportuno scegliere di affidarsi ad un tipo di cloud “private” o “hybrid” per poter integrare l'infrastruttura esistente con il nuovo modello operativo.

Un'impresa di grandi dimensioni, operante da tempo, che decide di adottare una private cloud, può permettersi di tagliare i costi legati al supporto tecnico e di incrementare l'utilizzo dei server a disposizione.

“Tipicamente l'impiego dei data center all'interno delle imprese “corporate” oscilla tra il 2% e il 10%. Decidendo di adottare una “private cloud”, questo livello può aumentare al 60% o al 70%, dando la possibilità all'azienda di evitare di investire denaro nell'acquisto di nuovi server”[6].

6 Michael H. Hugos, Derek Hulitzky, *Business in the cloud: what every business needs to know about cloud computing,* Wiley, Hoboken, 2010.

Un'impresa di questo tipo, però, nel caso in cui si trovi a dover fronteggiare un'ondata improvvisa e inaspettata di utilizzo, da parte di numerosi utenti, di una delle sue applicazioni, potrebbe scontrarsi con un problema di difficile risoluzione, in quanto l'ampliamento immediato della capacità dei server, tipico delle public cloud, non sarebbe attuabile.

Se, però, l'azienda suddetta avesse precedentemente scelto una “hybrid cloud”, il potenziale disguido non avrebbe ragione di esistere. Essa, infatti, potrebbe beneficiare delle precedentemente citate potenzialità della “public cloud”, espandendo immediatamente (e a basso costo) la capacità dei propri server e ovviando, così, istantaneamente, al problema.

1.8 La “private cloud” é davvero l'opzione più adatta per la sicurezza dell'azienda?

Precedentemente si é discusso dello scetticismo di molti manager di fronte ai potenziali problemi di sicurezza che derivano dall'affidare i propri dati ad un soggetto esterno (problemi dovuti al timore che, alcuni suoi componenti, possano averne accesso senza autorizzazione).

In realtà, i pericoli principali provengono, spesso, da soggetti terzi, visto e considerato che non é nell'interesse del fornitore dei servizi di cloud computing

adottare comportamenti che ne possano ledere l'immagine e incidere, quindi, sui suoi guadagni e, di conseguenza, sulla sua sopravvivenza.

Considerato questo aspetto, vi sono tre principali motivi per i quali le “public cloud” vengono ritenute le più sicure:

1) hanno meccanismi di difesa estremamente sviluppati, forgiati da frequenti attacchi da parte di innumerevoli hacker (le “public cloud” si trovano, nella quasi totalità dei casi, a gestire un cospicuo ammontare di dati sensibili, che attraggono l'interesse di svariati soggetti esterni, i quali cercano di averne accesso seppur non autorizzati. Questi continui tentativi di intrusione obbligano i provider ad essere sempre all'avanguardia nei metodi e nelle tecniche necessari a fronteggiarli).

2) attirano e, quindi, hanno a disposizione i migliori esperti in termini di sicurezza “sulla piazza” (dove gli attacchi sono più frequenti e più difficili da “disinnescare” e dove i dati sono più confidenziali, la necessità di personale altamente qualificato e i corrispettivi salari sono giustificatamente più elevati; é normale, perciò, che i migliori elementi specializzati nella lotta agli hacker finiscano per fare parte di questo tipo di organizzazioni).

3) sono sempre al passo con la tecnologia e possiedono i migliori dispositivi di sicurezza sul mercato (a differenza delle “private cloud” in cui spesso

l'azienda, per non essere costretta a continuare a spendere denaro nel "security hardware" dotandosi, quindi, degli strumenti più aggiornati e recenti, si accontenta di soluzioni più obsolete).

A questo va aggiunto che, nella gran parte dei casi, la formazione interna dello staff delle "private cloud", adibito al funzionamento e monitoraggio dei servizi IT, non consente di ricreare figure mediamente della stessa competenza di quelle facenti parte delle soluzioni "public".

Ne consegue che la presenza di queste lacune, non semplici da colmare, potrebbe portare a pesanti ripercussioni sia in termini di performance, sia in termini di sicurezza dei dati contenuti nella cloud stessa.

1.9 La diffusione capillare e le prospettive future

Un sempre più crescente e rilevante numero di imprese si sta accorgendo, di giorno in giorno, delle potenzialità del cloud computing e lo sfruttamento delle sue soluzioni sta divenendo un requisito fondamentale per ottenere vantaggi in termini di risparmio di costo e tempo e per avere a disposizione i migliori servizi IT presenti sul mercato. Come vedremo qui di seguito, anche la Commissione Europea e le organizzazioni governative di alcune tra le più importanti nazioni mondiali ne hanno intuito il grande potenziale, così come i Paesi in via di sviluppo hanno capito che potrebbe

rappresentare una risorsa, a dir poco rilevante, per il loro processo di crescita in pieno svolgimento.

La naturale conseguenza sarà una costante e continua impennata nell'utilizzo di questo tipo di servizi su scala mondiale; un utilizzo destinato ad aumentare di anno in anno, di cui, al momento, non si riescono ad immaginare i limiti.

1.9.1 Gli incentivi offerti dall'Europa alla crescita del cloud computing

La Commissione Europea, accortasi delle grandi potenzialità del cloud computing e degli enormi benefici che la sua adozione comporta, si é orientata verso un piano di appoggio alla diffusione di piattaforme cloud che, se portato a compimento con successo, si stima che avrà come conseguenza un investimento di 45 bilioni di euro addizionali di spesa diretta in servizi cloud e la creazione di 3,8 milioni di posti di lavoro extra, entro il 2020.

Tutto questo tenendo, ovviamente, in considerazione gli ostacoli possibili che tale propagazione su suolo europeo potrebbe trovarsi a fronteggiare; tra essi, il più evidente é sicuramente quello dovuto alla frammentazione del mercato dovuta alle differenti strutture legislative da Stato a Stato, che rendono complicato l'utilizzo di servizi cloud che “abbraccino” più giurisdizioni.

Raggiungere una posizione comune in “aree” come la privacy dei dati, i contratti e le norme di protezione per il consumatore, é, infatti, una sfida per nulla facile da

affrontare.

Il piano di sostegno pensato dalla Commissione, funzionale alla "dilatazione" dei servizi cloud su larga scala, si articola in tre passaggi fondamentali:

- *Spinta all'adesione a standard specifici da parte dei provider:* la Commissione crede fermamente che una vasta adesione a specifici standard (in nome dell'uniformità), connessi a certificati che attestino che i servizi cloud rispettano tali requisiti, aiuterà ad accelerare il tasso di adozione del cloud computing su scala europea.

  Per arrivare a ciò, però, si dovrà inevitabilmente scontrare con alcuni cloud provider che, per paura di perdere i propri clienti, si opporranno ad ogni tentativo di creare un'industria di servizi standardizzata che possa sfociare, quindi, in una variazione del loro "status quo".

- *Spinta alla stipula di contratti sicuri ed equi:* solitamente, i contratti per la fornitura di servizi cloud vengono stipulati seguendo un procedimento nel quale l'impresa-cliente determina quali prestazioni, tra quelle proposte dal provider, richiede per lo svolgimento dei propri processi di business, ma con poco spazio dedicato alla determinazione delle condizioni contrattuali da applicare. Questa mancanza spiega il fatto che i contratti per la fornitura di servizi cloud siano spesso sbilanciati a favore del provider, non fornendo adeguate garanzie di copertura su importanti elementi quali, ad esempio, la

responsabilità nella salvaguardia dell'integrità dei dati e la continuità del servizio.

E' intenzione, quindi, della Commissione lanciare una proposta comune che superi le divergenze legislative delle diverse nazioni, fornendo modelli contrattuali a cui uniformarsi, dotati di un insieme di regole ben definite da seguire. Il fine é quello di identificare termini e condizioni contrattuali sicure ed eque, per tutelare l'insieme di clienti che si rivolgono al cloud computing, con particolare focus ai segmenti più deboli quali i singoli consumatori e le piccole imprese.

- *Promuovere la leadership del settore pubblico:* considerando che il settore pubblico rappresenta il primo acquirente di servizi IT in Europa, il suo ruolo nella diffusione del cloud computing potrebbe divenire rilevante, se si creasse un fronte comune di requisiti richiesti ai provider in termini di performance e sicurezza.

  Per questo motivo, la Commissione ha deciso di creare un organo chiamato "European Cloud Partnership" (ECP) adibito a stimolare la collaborazione di esperti dell'industria e membri del settore pubblico dei vari Stati, per offrire un servizio di "public cloud" sicuro ed in linea con le regole europee in termini di protezione dei dati. (-Alistair Maughan, *"Europe offers incentives to cloud computing growth"*, Intellectual Property & Technology Law Journal, 2013-)

1.9.2 Anche le organizzazioni governative optano per l'uso di piattaforme cloud

Vista l'importanza che il cloud computing sta assumendo a livello mondiale e gli effettivi vantaggi che possono scaturire da un suo adeguato utilizzo, anche le organizzazioni governative hanno cominciato, copiosamente, a beneficiarne.

I governi che sono intenzionati a servirsi di questo tipo di tecnologia devono, però, focalizzarsi preventivamente su tre obiettivi principali:

- *Assicurare la sicurezza dei propri dati:* trattandosi di dati governativi, gli elementi riguardanti la sicurezza e la privacy degli stessi vanno considerati con la dovuta attenzione e scrupolosità.

- *Superare lo scetticismo di coloro che vedono il cloud computing come un rischio:* il governo deve essere capace di vincere le resistenze interne dei "tradizionalisti" che vedono l'adozione di tecnologie cloud, specialmente per quanto riguarda l'affidamento di importanti dati ad un terzo, come una scelta rischiosa.

  In realtà, come sostenuto anche dall'amministrazione Obama, l'affidamento ad un cloud provider può migliorare sensibilmente la performance del governo e tagliare considerevolmente i costi, grazie al trasferimento dei programmi IT all'interno di una struttura gestita da terzi.

- *Incoraggiare i fornitori di servizi cloud ad essere trasparenti in merito al loro operato:* aspetto fondamentale e per nulla trascurabile é il rapporto di fiducia che é necessario che si crei tra il governo e il provider a cui questi si rivolge. Da tale tipo di rapporto, infatti, dipenderà gran parte della buona riuscita dell'accordo stipulato per la fornitura dei servizi.

  Un ottimo punto di partenza é sicuramente, quindi, una gestione operativa all'insegna della trasparenza da parte del provider in questione; in tal modo, il governo avrà la facoltà di poter monitorare in modo completo, in qualsiasi momento, le attività svolte dalla controparte, ponendo, così, le premesse per la creazione di un rapporto solido e duraturo. (-Daniel Burton, *"What cloud computing means for government"*, Government News, 2012-) (-Reuven Cohen, *"The past, the present, and the future of cloud computing"*, Intel Technology Journal, 2012-)

1.9.3 Il cloud computing nei Paesi in via di sviluppo

L'avvento del cloud computing costituisce anche un'enorme opportunità per i Paesi in via di sviluppo, che possono benificiare di servizi già "preconfezionati", elastici e scalabili. Questo tipo di servizi permettono di sopperire allo svantaggio economico e tecnologico tipico di tali nazioni, rendendole capaci di risolvere problemi interni e di diventare protagonisti nella scena competitiva internazionale. (-Samuel Greengard,

"Cloud computing and developing nations", Communications of the ACM, 2010-) Ora, nel dettaglio, analizziamo le varie sfaccettature connesse, appunto, all'introduzione delle tecnologie cloud nei Paesi in via di sviluppo.

Innanzitutto partiamo esaminando le *implicazioni* direttamente collegate all'avvento del cloud computing:

- *Miglioramenti nella produttività e nell'efficienza operativa:* analisi effettuate in paesi come Cina, India e Sud Africa, hanno evidenziato che l'adozione di servizi su piattaforme cloud ha portato ad un notevole miglioramento nella produttività delle imprese e ad una considerevole riduzione dei costi.

- *Accrescimento della sicurezza nel settore IT:* il modello del cloud computing, grazie alle economie di scala su cui si fonda, é in grado di offrire un genere di business nel quale i clienti possono integrare i propri dati e le corrispettive applicazioni usufruendo di strutture esterne. Non solo, tali strutture esterne sono rinomate anche per essere all'avanguardia in ambito di sicurezza oltre che per risultare accessibili a costi modici.

  Questo insieme di elementi, ha permesso a molte aziende di Paesi in via di sviluppo di sopperire ai "deficit" di abilità ed esperienza dei propri dipendenti in tema di information technology e di superare una parte consistente dell'arretramento tecnologico caratterizzante i macchinari e la gestione operativa.

- *Sviluppo di nuovi prodotti e servizi:* la possibilità di giovarsi dei servizi cloud ha consentito ad innumerevoli start-up e imprese delle cosiddette “nazioni del sud del mondo” di trovarsi nella condizione di poter rendere effettive idee e relativi progetti di nuovi prodotti e servizi da lanciare sul mercato che, in molti casi, si sono rivelati utili per l'intera popolazione.

- *Possibilità di raggiungere nuovi mercati:* il cloud computing si dimostra un prezioso alleato delle piccole/medie imprese. Grazie ad esso, infatti, queste ultime possono trovarsi nella condizione di annullare il “gap” tecnologico e monetario nei confronti delle grandi imprese internazionali e proporre i propri prodotti/servizi su scala mondiale, entrando in diretta competizione con esse. Nei Paesi del terzo mondo, in cui questo tipo di imprese rappresenta la regola, questo é un aspetto di non poco conto da tenere in considerazione.

- *Opportunità di esportare servizi cloud:* un'ulteriore fonte di guadagno può essere la possibilità di esportare applicazioni e servizi basati su tecnologie cloud. Opportunità che molte medio/piccole imprese hanno deciso, giustamente, di cogliere al volo.

Ora prendiamo in considerazione le *determinanti* che influenzano la diffusione dei sistemi cloud nei Paesi in via di sviluppo:

- *Sviluppo delle strutture e dei servizi di supporto ad esse correlate:* l'impiego e la diffusione del cloud computing dipendono sicuramente dalla presenza di un livello di sviluppo accettabile dei vari settori fondamentali alla base di una società civile. La presenza di un sistema sanitario ed educativo di base, ad esempio, genera la domanda dei relativi servizi che da essi derivano; in questo contesto, l'adozione di soluzioni cloud sarebbe più che giustificata e porterebbe a concreti vantaggi per l'intera popolazione.

  Le soluzioni cloud, quindi, rappresentano una grande opportunità per i Paesi più arretrati, ma il loro stato di "arretratezza" non deve essere di livello troppo elevato; se così fosse, i pochi presupposti richiesti dal cloud computing verrebbero a mancare e la sua diffusione non potrebbe avvenire.

- *Supporto istituzionale e legislativo:* il supporto istituzionale e legislativo all'introduzione del cloud computing é essenziale. La propagazione di questo tipo di servizio é, infatti, dipendente dal livello prioritario assegnato dal governo di ogni nazione a questo tipo di settore e dalle politiche instaurate per incoraggiarne l'eventuale adozione.

La diffusione dei servizi cloud nei paesi in via di sviluppo é destinata a crescere sempre di più. Al contrario dei paesi più sviluppati che, prima dell'avvento del cloud

computing, si sono dovuti dotare di data center interni e delle competenze necessarie per farli funzionare al meglio, essi, infatti, hanno la fortuna di poter saltare questa fase.

I servizi cloud, inoltre, sono accessibili da ogni dispositivo dotato di connessione internet; questo rende possibile l'utilizzo di telefoni cellulari a basso costo e di facile reperibilità anche per i meno abbienti, evitando, quindi, l'obbligo di dover acquistare un personal computer, spesso, in questi Paesi, non economicamente alla portata. (-Nir Kshetri, *"Cloud computing in the global south: drivers, effects and policy measures"*, Third World Quarterly, 2011-)

1.9.4 I dati attuali e l'evoluzione prospettica

I dati attuali riguardanti l'adozione del cloud computing a livello mondiale e le stime stilate per il futuro, ci danno un'idea di come esso si stia diffondendo "prepotentemente" andando a costituire un vero e proprio fattore indispensabile, nella maggior parte dei casi, per poter competere con la concorrenza "ad armi pari".

A testimonianza di tutto ciò, é stato rilevato che, già nel 2012, il 90% delle organizzazioni mondiali ha valutato attentamente l'eventualità di dotarsi di soluzioni cloud (spesso finendo per adottarle), andando a costituire un incremento effettivo del 75% rispetto all'anno precedente.

Dando un'occhiata a ciò che accadrà nel futuro, il trend é destinato a crescere in maniera decisa; ci si aspetta, infatti, che il mercato riguardante i servizi cloud si

espanda del 44% annuo da oggi al 2016, quando é previsto che esso rappresenterà il 60% dell'intero traffico mondiale connesso ai data center. (-Eunjeong Choi, *"How cloud computing is revolutionizing the future"*, Seri Quarterly, 2013-) La diffusione del cloud computing su scala globale, seppur già notevolmente estesa, é solamente agli albori e non ha nessuna intenzione di arrestarsi.

Capitolo 2

BENEFICI E RISCHI LEGATI AL CLOUD COMPUTING

2.1 Gli elementi principali che spingono le aziende ad affidarsi al cloud computing

Sono molteplici le ragioni che spingono le imprese, al giorno d'oggi, ad avvicinarsi al mondo delle piattaforme cloud, rendendole parte integrante del proprio percorso strategico e operativo. Il cloud computing, infatti, é divenuto ormai un servizio tra i più determinanti a fini di mantenimento/raggiungimento del vantaggio competitivo, viste le implicazioni che un suo utilizzo comporta.

Qui di seguito ne analizziamo le più importanti:

- *Possibilità di convertire costi fissi in costi variabili:* adottare servizi cloud permette all'impresa di convertire i tradizionali costi fissi, che derivano dall'acquisto e manutenzione di un data center, in costi variabili, dovendo pagare solo l'ammontare di risorse IT effettivamente utilizzate. (-Zhang Ling, Gu Wenlin, "*The simple analysis of impact on financial outsourcing because of the rising of cloud accounting",* Asian journal of business management, 2013-)

  Se, quindi, i costi fissi legati all'acquisto dei server (che a fini contabili vanno a comporre il cosiddetto "ammortamento" e, cioé, vengono sottratti, cumulativamente e in base alla vita utile della macchina, ad ogni bilancio d'esercizio) rimangono costanti a prescindere dalle vendite che l'azienda riesce ad ottenere, così non é per quelli variabili che dipendono direttamente dai profitti realizzati. Questo permette all'impresa di variare l'utilizzo di servizi IaaS, PaaS o SaaS in base all'andamento del volume delle vendite e dell'output realizzato e di avere un impatto positivo anche sul "cash flow"[7]. (-Ceslovas Christauskas, Regina Miseviciene, *"Cloud computing based accounting for small to medium sized business"*, Engineering Economics, 2012-)

  Per concludere, va messo l'accento sul fatto che, in questo modo, l'impresa riesce a scaricare sul provider il cosiddetto <rischio di "picchi" di utilizzo dei server>, cioé l'onere di garantire la normale operatività anche in contesti nei

7 "*Cash flow*": quando si parla di "cash flow", "flusso di cassa", si fa riferimento ai flussi monetari (differenza tra entrate ed uscite monetarie) di un'azienda in un determinato periodo di riferimento. Il suo ammontare é, quindi, importante (e, per questo va adeguatamente monitorato) per far fronte ad eventuali esigenze/spese a breve termine o anche ad opportunità legate ad investimenti particolarmente vantaggiosi.

quali vi é uno sfruttamento elevato dei servizi offerti, in seguito all'accesso contemporaneo da parte di più utenti alle strutture hardware e alle connesse applicazioni software, messe a disposizione.

Uno dei più grandi problemi che si riscontrano, infatti, al momento dell'acquisto del data center é quello di acquisirne uno tale da sopperire ad eventuali casi di sovrautilizzo. Questo porta all'acquisto di macchinari che si trovano, quindi, enormemente sottoutilizzati per la maggior parte della propria vita utile.

Aderendo ai servizi cloud, anche questo problema svanisce e viene trasferito all'esterno (nello specifico, come detto, al provider che sopperisce al problema degli sprechi connessi al sottoutilizzo dei server aziendali, grazie al meccanismo della "virtualizzazione dei server"[8], che ne permette un uso condiviso tra più utenti).

- *Opportunità di realizzare un ROA[9] nettamente più elevato:* considerando che il ROA indica quanto l'azienda riesce a guadagnare per ogni dollaro investito, le compagnie che sono costrette ad effettuare un notevole investimento iniziale in data center, registreranno un valore più basso di questo indice rispetto a quelle che optano per delle soluzioni cloud (in cui questo tipo di spese non sono necessarie, visto e considerato che i data center sono di proprietà di un soggetto terzo che si occupa anche del loro funzionamento). In quest'ultimo caso,

8 "*Virtualizzazione dei server":* vedi Capitolo 1, pag. 14.
9 "*ROA"*: "Return On Assets", cioé un indice di bilancio che misura la redditività del capitale investito. Si calcola come segue: (reddito netto – oneri finanziari)/totale dell'attivo.

quindi, le imprese si troveranno nella situazione di poter usufruire di una quantità di capitale in più da destinare ad altri fini aziendali.

- *Maggiore agilità di business e miglioramento del "time to market":* il cloud computing, in risposta a qualsiasi nuova esigenza di business, offre la possibilità di fare uso di risorse IT [come intere infrastrutture (IaaS), piattaforme software (PaaS) e applicazioni (SaaS)] già pronte per l'utilizzo, consentendo, così, di raggiungere un'elevata agilità di business e un netto miglioramento del "time to market". Tutto questo, quindi, senza l'impegno di dover acquistare, installare, configurare e monitorare personalmente il funzionamento delle predette componenti.

  Le risorse, in questo modo, saranno disponibili nel giro di poche ore dal momento del bisogno (invece delle consuete settimane o mesi che accompagnano un'acquisizione interna), semplicemente dietro pagamento con carta di credito ad un provider esterno, permettendo, da subito, di poter lavorare sullo sviluppo e la realizzazione del prodotto.

  Ciò permette una penetrazione del mercato immediata e consente di sfruttare i vantaggi competitivi del prodotto anticipando i concorrenti (viene ottenuta, quindi, una <riduzione del "time to market">).

  Per ciò che concerne l'agilità di business, invece, le soluzioni cloud permettono alle aziende di effettuare delle sperimentazioni in merito alla creazione di un nuovo prodotto o servizio e vederne gli sviluppi. Se, poi, si riterrà conveniente

proseguire nella realizzazione dello stesso, si effettueranno ulteriori investimenti cloud, altrimenti si terminerà istantaneamente; questa caratteristica vincente del cloud computing é detta “scalabilità”. L'impresa che decidesse di non beneficiarne, sarà costretta ad acquisire tutte le risorse strutturali necessarie per la realizzazione dell'idea di business, con l'obbligo di procedere nel pagamento complessivo delle stesse anche dopo un eventuale negativo riscontro iniziale, che consiglierebbe un abbandono repentino del progetto in fase di svolgimento. (-Fatima A. Alali, Yeh Chia-Lun, “*Cloud computing overview and risk analysis”*, Journal of information systems, 2012-) Si tratta, quindi, di importantissimi elementi da considerare per qualsiasi tipo di azienda, ma sicuramente fondamentali per ogni singola start-up, che potrà testare e, conseguentemente, sviluppare la propria idea di business, diffondendola sul mercato in tempi brevi e senza proibitivi investimenti iniziali in strutture IT. (-R. Von Solms, M. Viljoen, “*Cloud computing service value: a message to the board”*, South African journal of business and management, 2012-)

- *Elasticità:* il provider di servizi cloud, sapendo della difficoltà che si verifichi che ogni utente si serva dei suoi servizi al massimo delle rispettive possibilità e nello stesso istante, indirizza i suoi investimenti iniziali in hardware e software mirando a fornire una capacità tale da sopperire al più alto picco medio di utilizzo previsto da parte dei suoi clienti. Il contemporaneo uso dei servizi del

fornitore, tipico del cloud computing, permette, quindi, di rispondere alle richieste dei clienti in maniera elastica, dando un'effettiva impressione, a ciascuno di essi, di poter beneficiare di un server dal contenuto illimitato. (-Jason Bloomberg, "*Wiley CIO: agile architecture revolution: how cloud computing, REST-based SOA and mobile computing are changing enterprise IT"*, Wiley, Somerset, 2013-)

- *Disponibilità di forza lavoro supplementare:* tale vantaggio risiede nella possibilità, attraverso il cloud computing, di affidare ad un soggetto esterno la realizzazione e la cura dei servizi SaaS, PaaS e IaaS, consentendo di poter avere a disposizione lo staff, solitamente adibito al funzionamento e al monitoraggio dei componenti IT all'interno dell'impresa, per altri importanti fini. Questa forza lavoro potrà, quindi, dedicarsi al perseguimento di ulteriori iniziative aziendali (sviluppo di nuove strategie, realizzazione di nuove idee di business, ricerca e sviluppo, innovazioni di prodotto e di processo, ecc.) portando un cospicuo valore aggiunto nel raggiungimento dell'output prefissato.

- *Considerevole risparmio di tempo e denaro per il settore HR*[10]*:* le imprese sono costrette ad investire elevate quantità di tempo e denaro per la formazione e il continuo aggiornamento dei dipendenti in merito alle tematiche IT, al fine di avere sempre personale idoneo per ciò che concerne la gestione dei sistemi

10 "Human Resources"

software presenti nell'organizzazione.

Con l'avvento del cloud computing, questo stanziamento di risorse non sarà più necessario, in quanto tali oneri rientreranno, automaticamente, all'interno dei servizi offerti dal provider.

- *Possibilità di rispondere celermente a repentini cambiamenti del mercato:* considerando che gran parte del successo di un'impresa dipende dalla sua capacità di soddisfare i gusti dei consumatori e di fronteggiare adeguatamente i propri concorrenti, essa é impegnata quotidianamente in un attento "scandagliamento" del mercato in cui opera.

  Per questo motivo, un'azienda operante all'interno di una piattaforma cloud, potrà usufruire dei servizi in essa contenuti per rispondere in tempo reale a nuove esigenze di prodotto o a minacce provenienti dal mondo dei "competitor"; tutto ciò, infatti, risulta realizzabile grazie ai vantaggi in termini di agilità di business e riduzione del "time to market" (precedentemente citati) che caratterizzano il mondo del cloud computing.

- *Presenza costante di patch*[11] *a protezione delle applicazioni di cui si fa uso:* l'installazione continua di patch aggiornate consente al sistema informatico di proteggersi dagli attacchi degli hacker, tanto più pericolosi, tanto più sono sensibili i dati che si intende salvaguardare.

  Mentre, però, affidandosi al cloud computing, il processo di inserimento delle

11 *"Patch":* aggiornamenti installati all'interno di un software mirati a correggere errori di programma e a fornire protezione da attacchi hacker.

patch e il loro divenire operative contro attacchi esterni é pressoché immediato, così non é per le aziende che decidano di affidarsi a soluzioni interne.

Una semplice indagine statistica é in grado di rendere meglio il concetto: "N*el 2003, al tempo delle prime statistiche al riguardo, venne rilevato che il tempo necessario per dotare di patch adeguate e operative metà del proprio sistema software, era di 30 giorni.*

Nel 2008, la medesima ricerca, ha potuto constatare la riduzione del lasso di tempo di sola mezza giornata (29,5 giorni). Questo consente agli hacker di avere a disposizione un mese circa per poter compiere i propri attacchi avvantaggiandosi delle macchine non dotate di patch"[12].

- *Possibilità di usufruire di piattaforme condivise per unire fruitori con scopi comuni:* le piattaforme cloud permettono un utilizzo condiviso a soggetti animati da fini e interessi comuni. Questi ultimi possono, quindi, collaborare allo sviluppo/risoluzione di progetti o semplicemente fornire idee e consigli che possano rivelarsi di mutuo interesse.

  Un esempio di questo tipo di servizio é tipicamente costituito da "Microsoft SharePoint" che offre, appunto, spazi di condivisione e interazione fra più utenti.

12 Kevin T. McDonald, *Above the clouds: managing risk in the world of cloud computing,* IT Governance, Cambs, 2010

- *Possibilità di accedere ai servizi cloud con un gran numero di tipi diversi di dispositivi e pressoché da qualsiasi luogo:* l'insieme dei servizi cloud sono accessibili dal cliente indipendentemente dal dispositivo utilizzato (che potrà essere un PC, ma anche un iPad o uno smart phone) e dal luogo da cui vi si vuole accedere per farne uso. (-Harry Katzan Jr.,*"On an ontological view of cloud computing",* Journal of Service Science, 2010-)

  L'unico requisito é, ovviamente, in entrambi i casi, una connessione internet attiva.

- *Possibilità di usufruire di servizi sempre all'avanguardia:* il provider si cura costantemente di offrire i migliori servizi disponibili sul mercato e di procedere ad un loro ripetuto e scrupoloso controllo.

  Da questa attenta e ripetuta analisi deriva uno sviluppo continuo degli stessi attraverso l'installazione tempestiva di aggiornamenti di vario genere.

  (-Christopher Yoo, *"Cloud computing: architectural and policy implications"*, Review of industrial organization, 2011-)

- *Risvolti ecologici:* la responsabilità sociale dell'impresa, in un contesto attuale caratterizzato da una indispensabile e dovuta attenzione alle problematiche ambientali, é un aspetto di determinante importanza e funge, sempre più, da fattore discriminante in termini di immagine agli occhi della clientela.

  Per questa ragione, l'adesione al "mondo" del cloud computing é senza dubbio la soluzione migliore a cui pensare; esso, infatti, permette di poter operare da

ogni luogo, usufruendo di server “virtuali” che permettono di evitare gli enormi dispendi di energia dei data center interni all'azienda e i problemi connessi allo smaltimento di quelli tra essi divenuti obsoleti (o solo di alcune parti di essi per cui si é resa necessaria una sostituzione).

Questo tipo di cambiamenti (un altro da considerare può essere quello che, considerata la possibilità di accedere a servizi cloud da ogni luogo e con ogni dispositivo avente una connessione internet, spesso i dipendenti decidono di lavorare da casa, riducendo rimarchevolmente il numero di automobili attive e i realtivi gas di emissione) porta a tangibili miglioramenti in termini di diminuzione dell'inquinamento e, quindi, anche di raggiungimento di una buona reputazione aziendale. (-Bose Indranil, *“Cloud computing and its impact on corporate HR practices”,* Advances in management, 2012-)

2.2 I rischi correlati all'uso di piattaforme cloud e come agire per fronteggiarli

Un potenziale cliente, completamente “agnostico” in tematiche cloud, che leggesse il precedente paragrafo, potrebbe incorrere nell'errore di considerare il mondo della “nuvola” come un vero e proprio paradiso fatto solo di vantaggi.
Così non é. Esistono, come é normale che sia, dei rischi organizzativi, operativi, tecnici e legali che vanno ponderati con attenzione.

Esempi di rischi caratteristici del cloud computing sono:

- *Sicurezza e privacy dei propri dati:* il soggetto che si indirizza verso soluzioni cloud, nella maggior parte dei casi, non si trova nella situazione di poter conoscere nel dettaglio i metodi operativi e le altre componenti legate alla struttura e all'organizzazione del fornitore del servizio.

  Per questo motivo ci si aspetta che il provider, a cui ci si affida, fornisca garanzie adeguate in termini di sicurezza e privacy dei dati che si intende “affidargli”[13].

  Se così non fosse la transizione in atto, che spinge sempre più aziende all'uso di piattaforme cloud, potrebbe subire un immediato (e potenzialmente irreversibile) rallentamento.

13 Nel quarto capitolo le tematiche della sicurezza e della privacy dei dati, dell'azienda che decide di adottare soluzioni cloud, verranno analizzate più nel dettaglio.

Il rischio che soggetti terzi (anche facenti parte dello staff del provider) accedano a dati sensibili aziendali sarebbe, infatti, troppo elevato e non giustificherebbe l'investimento.

Da ciò deriva il fatto che la scelta del provider, come vedremo in seguito, sia una tappa fondamentale nell'adozione di servizi cloud.

- *"Vendor lock-in":* quando si parla di "vendor lock-in" si fa riferimento al rischio di rimanere "bloccati" nel rapporto, una volta stipulato il contratto con il provider.

  Considerando che i sistemi cloud si basano, in buona parte, su architetture software differenti da quelle che l'azienda utilizzava (o avrebbe utilizzato, nel caso di una start-up che si affida fin dall'inizio del proprio operare al cloud computing) al suo interno prima della transizione, quando il cambiamento sarà avvenuto risulterà difficile tornare alla soluzione precedente o rivolgersi ad un altro provider.

  Tale passo, infatti, potrebbe risultare proibitivo per l'azienda sia in termini di tempo, sia, soprattutto, in termini di esborso monetario necessario.

  Per queste ragioni, per evitare spiacevoli sorprese, prima di scegliere il cloud provider va fatta un'attenta analisi sulla longevità e la stabilità della società che questi presiede e sui costi, in ottica prospettica, che derivano dal godimento dei servizi da esso offerti.

- *I cambiamenti da effettuare all'interno dell'azienda per accogliere soluzioni cloud possono generare del malcontento:* come diretta conseguenza del passaggio da una struttura interna ad una che usufruisce di servizi cloud, vanno effettuati dei cambiamenti specifici all'interno dell'azienda. Questi cambiamenti, riguardanti la struttura, ma soprattutto le mansioni e le rispettive responsabilità di parte dello staff, se non ponderati e affrontati con la dovuta attenzione, possono sfociare in malcontento e calo nella motivazione dei lavoratori stessi.

  All'azienda il compito di evitare che un simile problema, che avrebbe riscontri negativi sull'efficienza e l'efficacia delle prestazioni lavorative, si venga a verificare. (-Amab Dutta, Alex Peng Guo Chao, Alok Choudhary, "*Risks in enterprise cloud computing: the perspective* of IT experts", Journal of computer information systems, 2013-)

- *Potenziali momentanei imprevisti che possono occorrere al provider:* solitamente il fornitore di servizi cloud considera ampiamente ogni variabile in gioco, per evitare indesiderati problemi di inefficienza che lo porterebbero a danni di immagine di gravità inquantificabile.

  A volte, però, anche alcuni famosi provider si sono trovati a fronteggiare problemi inaspettati.

  "Amazon Elastic Cloud Compute", un servizio offerto da Amazon che consiste nella fornitura ai clienti di una piattaforma per ospitare siti web e applicazioni

varie, ne é un esempio. Nell'aprile del 2011 una parte di esso, destinata a soddisfare una porzione di utenti situati nella costa est degli Stati Uniti, é rimasta inattiva per svariati giorni. Seppure Amazon sia riuscita a recuperare la gran parte dei dati, alcuni andarono persi per sempre, costituendo un danno di portata elevatissima per i clienti e, di riflesso, per la reputazione della società stessa.

Nel settembre dello stesso anno, anche alcuni software di Microsoft adottanti tecnologie cloud (Hotmail, SkyDrive e Office 365) si trovarono nel bel mezzo di un inconveniente; rimasero, infatti, inattivi per circa 3 ore.

Per un'azienda che abbia deciso di dotarsi di tecnologie cloud, anche poche ore di inutilizzo possono rappresentare rilevanti perdite in termini di costi finanziari e operativi.

Per queste ragioni ogni azienda “devota” al cloud computing, oltre a prendere in considerazione adeguatamente queste possibilità al momento della stipula del contratto, dovrebbe affidarsi a più provider per poter, così, evitare ogni rischio e non dover “legare a doppio filo” i propri destini a uno di essi. (-James R. Kalyvas, Michael R. Overly, Matthew A. Karlyn, “*Cloud computing: a practical framework for managing cloud computing risk” (part 1)*, Intellectual Property & Technology Law Journal, 2013-)

- *La reputazione negativa di un cliente operante in una cloud può ledere anche quella degli altri:* se uno dei clienti che operano all'interno di una cloud mette in atto comportamenti opportunistici, immorali o, peggio, illegali, la conseguenza che ne deriva é che tali azioni possono ledere alla reputazione anche degli altri clienti operanti nella medesima.

  Nel marzo 2009, ad esempio, la Federal Bureau of Investigation (FBI) fece irruzione in un data center di Dallas, in quanto una delle compagnie che ne usufruiva era indagata per attività criminali. Un numero imprecisato di altre imprese, anch'esse facenti uso del medesimo data center ma senza alcun legame con l'impresa incriminata, si trovò a pagare ingiustamente le conseguenze di questa operazione, vivendo momenti di gravi perdite o, nei casi limite, di forzata uscita dal business.

  La reputazione negativa dell'impresa sotto investigazione aveva inciso anche sulla loro ineccepibile immagine di imprese in linea con i dettami imposti dalla legge. (-Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia, "*A view of cloud computing",* Communications of the ACM, 2010-)

2.3 I costi del cloud computing

I costi legati al cloud computing sono un fattore molto rilevante da analizzare; i manager, infatti, li tengono in notevole considerazione al momento della decisione tra comprare e far funzionare all'interno dell'azienda i componenti software e hardware necessari, o affidarsi ad un cloud provider esterno.

A tal riguardo, a livello generico, é possibile affermare che per i progetti a breve termine (fino a circa 2 anni) é quasi sempre più conveniente affidarsi ad una soluzione esterna, in quanto i costi legati all'acquisizione di server interni sarebbero decisamenti più elevati, mentre per ciò che riguarda piani strategici che superano i 2 anni, la soluzione esterna sembrerebbe, invece, rivelarsi sconveniente. Va, però, sottolineato che, raggiunti i 3 anni, spesso i macchinari vanno aggiornati (se non sostituiti interamente), ragion per cui sembra evidente che la soluzione cloud rimanga, a prescindere dall'investimento temporale, la migliore da adottare.

In molti casi, poi, al momento del confronto delle due soluzioni, le compagnie non considerano adeguatamente l'incidenza dei costi indiretti che pesano sulla scelta di una soluzione interna.

Esempi di questo genere di costi sono:

- *Costi del personale per la gestione dei sistemi hardware e software acquistati:* cioé i costi che derivano dalla necessità di possedere, all'interno dello staff, persone adibite al funzionamento, alla manutenzione e ai processi di aggiornamento dei servizi IT.

- *Elettricità, impianti di raffreddamento e costi di affitto:* si tratta dei costi legati strettamente ai server in termini di elettricità, impianti di raffreddamento e di affitto della stanza in cui vengono collocati.

- *Costi opportunità:* cioé gli esborsi in termini monetari e in termini di forza lavoro dedicata che, se ci si affidasse ad una soluzione esterna, potrebbero essere reinvestiti all'interno dell'azienda per fini connessi ad un miglioramento dell'output.

2.4 I fattori che portano l'azienda a sviluppare un modello cloud ottimale

Il successo di un'azienda che decida di affidarsi a soluzioni cloud, é conseguenza diretta di tre categorie principali di benefici che derivano da questo tipo di scelta: strategico (l'impresa può delegare ad un terzo le funzioni connesse all'IT e concentrarsi, così, sul proprio "core business"), economico (sfruttamento dell'esperienza, delle conoscenze e delle risorse tipiche dell'ambiente IT possedute dal provider, che consente di spendere molto meno rispetto alla necessità di sviluppare le stesse internamente all'azienda) e tecnologico (possibilità di eliminare il rischio di obsolescenza della tecnologia interna impiegata nei processi operativi, grazie alla capacità del provider di fornire le migliori soluzioni tecniche sul mercato e di procedere ad un continuo monitoraggio e aggiornamento delle stesse).
Visto e considerato, però, che i servizi legati al cloud computing sono accessibili e replicabili da più aziende, l'impresa che intende differenziarsi, conseguendo un vantaggio competitivo rispetto alle altre, deve essere in grado di generare capacità IT particolari e discriminanti.

A tal riguardo se ne possono individuare due tipi:

- *Capacità tecniche:* le capacità tecniche sono insite nei componenti hardware e software di cui l'azienda dispone. Tanto più esse sono sviluppate e moderne, tanto più risulterà semplice e, soprattutto, portatore di rilevanti economie di

scala e vantaggio competitivo, il passaggio e l'adattamento al cloud computing. Se, infatti, le caratteristiche tecniche aziendali sono adeguatamente flessibili e scalabili, la “traslazione” dall'interno all'esterno della gestione e operatività dei servizi IT avverrà in maniera più naturale ed efficiente e permetterà di arrivare ad una contrazione delle spese correlate più celermente rispetto agli altri concorrenti.

- *Capacità manageriali:* le abilità dei manager nel coordinare le attività che occorrono per realizzare il passaggio a soluzioni cloud sono fondamentali. Nello specifico, le organizzazioni dotate di manager di elevata competenza nell'ambito dell'information technology e con annesse radicate capacità di raggiungimento di proficui obiettivi economici, godranno della possibilità di saper scegliere i servizi cloud più consoni all'azienda e pertinenti alle strategie di business adottate. Da ciò deriva che, tanto più alte sono le competenze dei manager, tanto più accentuati saranno, per l'impresa, gli incrementi effettivi intermini di efficienza e capacità di realizzare lauti guadagni.

  Tutto questo operando all'interno di una visione, possibilmente, prospettica consentendo all'azienda, quindi, di beneficiare di soluzioni in grado non solo di portare esclusivamente vantaggi nell'immediato, ma anche di assicurare una continuità di risultati positivi che si rifletta anche negli esercizi futuri.

  Per arrivare a ciò, compito dei manager é cercare di anticipare i cambiamenti in divenire, arrivando a comprendere il prima possibile come le tecnologie

emergenti possano generare effetti sulla “business performance” aziendale nel tempo. (-Gary Garrison, Sanghyun Kim, Robin L. Wakefield, “*Success factors for deploying cloud* computing”, Communications of the ACM, 2012-)

Capitolo 3

LA SCELTA DEL CLOUD COMPUTING E I CORRISPETTIVI RISVOLTI AZIENDALI

3.1 Aspetti da considerare prima di avventurarsi nel cloud

La scelta di un'azienda di “avventurarsi” nel mondo del cloud computing, seppur sembri la più conveniente e naturale opzione da considerare, non va fatta frettolosamente. E' necessario, infatti, considerare vari aspetti ed implicazioni per poter decidere in maniera definitiva se si tratti di un'operazione in grado, effettivamente, di portare più vantaggi che svantaggi.

E' possibile suddividere le varie considerazioni da fare in due parti principali: quelle che riguardano gli aspetti interni all'organizzazione e quelle che vengono fatte rivolgendo il proprio sguardo esternamente e, quindi, principalmente verso il cloud provider a cui ci si intende rivolgere.

Considerazioni che derivano da un'analisi interna:

- *L'organizzazione é pronta, dal punto di vista culturale, a spostare le proprie strutture software, i propri dati, i propri processi e le proprie applicazioni all'interno di un sistema cloud?*

  Va fatta un'attenta analisi intraziendale per essere sicuri che l'organizzazione sia pronta, dal punto di vista culturale, alla transizione verso un sistema cloud, in modo da evitare resistenze interne al momento delle operazioni richieste per il cambiamento.

  In caso di buon esito si deve, poi, procedere a istruire dettagliatamente lo staff sui compiti, i doveri e le responsabilità che sopraggiungeranno al termine del cambiamento in atto. (-Hossein Bidgoli, *"Successful introduction of cloud computing into your organization: a six step conceptual model"*, Journal of international technology & information management, 2011-)

- *C'é la possibilità che, nel caso in cui le risorse IT, affidate ad un terzo, vengano gestite in maniera più efficace ed efficiente, queste contribuiscano in modo deciso al raggiungimento di un vantaggio competitivo?*

  Se ci si accorgesse che, affidando ad un terzo le proprie risorse IT, si potesse raggiungere un vantaggio competitivo dovuto alla maggiore efficacia ed efficienza con cui, quest'ultimo, le gestirebbe, un passo importante verso la scelta del cloud sarebbe stato fatto.

- *Quali sono i punti di forza e le principali variabili strategiche tipiche dell'impresa?*

  E' necessario procedere ad un'adeguata valutazione dei punti di forza e delle principali variabili strategiche dell'impresa, da cui possono derivare le scelte operative in termini di cloud computing.

  Se, infatti, gli elementi che si intende affidare in "outsourcing" fossero di vitale importanza per l'azienda dal punto di visto strategico, quest'ultima potrebbe convenire che, darli in gestione ad un terzo, potrebbe rappresentare un rischio troppo elevato, che non conviene correre.

- *Quali applicazioni aziendali beneficerebbero della conversione al cloud computing?*

  Se un'applicazione funziona bene, é usata solo da una manciata di persone e non necessita di aggiornamenti, può essere sconveniente traslarla all'interno di una piattaforma cloud.

  Ragion per cui, prima di procedere al cambiamento, si rende necessaria un'attenta analisi delle componenti IT presenti in azienda.

Considerazioni che derivano da un'analisi esterna:

- *Il cloud provider ha un "disaster recovery plan"*[14] *adeguato? Si é premurato di testarlo adeguatamente?*

  E' importante essere sicuri che, in caso di inaspettati problemi alle strutture IT demandate in gestione al provider, non vi siano rischi legati alla perdita dei dati in esse contenuti o interruzioni che non ne permettano l'utilizzo per lassi di tempo troppo lunghi. Se così non fosse, infatti, i danni economici per l'azienda, nel caso del sopraggiungere di tali inconvenienti, sarebbero di enorme entità. Per questo motivo sarebbe sempre meglio assicurarsi, ove possibile, che il cloud provider abbia un "disaster recovery plan" adeguato e premurarsi di chiedere di visionare i dati relativi all'ultimo test effettuato su di esso, per poter vedere con i propri occhi l'attendibilità/affidabilità del piano. (-Brian J. Tsai, John Shen, *"Securities operations: in-house or in the cloud"*, Journal of securities operations & custody, 2012-)

- *Il provider con cui interagiremo si può considerare affidabile? Quanta esperienza possiede nella fornitura dei servizi a cui é dedicato?*

  E' sempre utile fare un'analisi della storia che caratterizza l'operato del fornitore di servizi cloud, scelto per una potenziale collaborazione: ricerca sui clienti precedenti, feedback di quest'ultimi sul rapporto avuto con esso, anni di

14 *"Disaster recovery plan":* quando si parla di "disaster recovery plan" si fa riferimento al processo comprendente l'insieme di procedure per riportare a regime le funzioni caratteristiche e proteggere i dati contenuti in un'infrastruttura IT di un'azienda, in caso di sopraggiunti problemi operativi.

operatività alle spalle, ecc...

In tal modo ci si può fare un'idea più precisa sull'affidabilità del provider e sulla sua capacità di offrire servizi di qualità, in tempi ridotti e in linea con le richieste.

- *I servizi offerti dal provider seguono fedelmente i precetti del cloud computing (velocità, semplicità e flessibilità)?*

  E' bene, ovviamente, che il provider scelto sia tra i migliori per qualità e caratteristiche intrinseche (tra le quali velocità, semplicità e flessibilità sono le più importanti) dei servizi proposti.

- *Quanto spesso il provider rende momentaneamente inutilizzabili i servizi cloud per dedicarsi alla loro manutenzione e al loro aggiornamento?*

  Naturalmente un'adeguata attenzione alla manutenzione e all'aggiornamento dei servizi offerti rappresenta una caratteristica positiva del provider in questione, in quanto sintomo di affidabilità e scrupolosità.

- *Che strategia di uscita dalla relazione con il provider abbiamo pianificato nel caso il rapporto si deteriorasse?*

  E' importante prevedere ogni eventuale risvolto e, quindi, anche quello di una malaugurata, ma necessaria, interruzione del rapporto con il fornitore dei servizi cloud. A tal proposito occorre dotarsi di un piano di via d'uscita tempestiva, in caso di sopraggiunto bisogno, per evitare il rischio di "lock in"[15].

15 *"Vendor lock-in":* vedi Capitolo 2, pag.53.

Piano d'uscita che sarebbe bene prevedesse, se i termini del contratto lo contemplano, anche la restituzione dei dati e l'eliminazione degli stessi dalle piattaforme del provider.

- *Il provider si appoggia ad altri partner nella fornitura del servizio?*

  Se il provider si appoggia ad altri partner nella fornitura dei servizi cloud, é dovere dell'azienda procedere ad un'analisi attenta e dettagliata anche dei loro profili.

- *E' possibile instaurare un rapporto a lungo termine con il provider Quest'ultimo gode di una buona salute finanziaria?*

  In ottica strategica, il passaggio all'adozione di soluzioni cloud viene quasi sempre adottato all'interno di una visione a lungo termine. Meglio, perciò, assicurarsi che il provider goda di una buona salute finanziaria, tale da poter sostenere una possibile relazione duratura.

- *Di che capacità di innovazione é dotato il provider?* Meglio scegliere un provider dall'elevata capacità innovativa. Sarebbe a dir poco sconveniente imbattersi in una situazione in cui l'azienda si trovi a sviluppare un nuovo prodotto all'avanguardia, ma il cloud provider non sia in grado di fornire i servizi richiesti per introdurlo sul mercato. (-Hunter Muller, *"On top of the cloud: how CIOs leverage new technologies to drive change and build value across the enterprise"*, Wiley, Hoboken, 2011-)

3.2 Il cloud adoption lifecycle

Una volta che l'impresa ha definitivamente scelto di entrare nel mondo del cloud computing, é possibile proseguire nelle varie fasi per rendere tale scelta effettiva; la sequenza di passi necessari per procedere con successo al cambiamento voluto costituiscono il cosiddetto “cloud adoption lifecycle”.

Si possono individuare quattro passaggi principali nella realizzazione del “cloud adoption lifecycle”:

- La fase della scelta del tipo di strategia da adottare
- La fase della scelta del provider e del tipo di cloud
- La fase del testing
- La fase dell'azione concreta

3.2.1 La fase della scelta del tipo di strategia da adottare

Il primo passo da affrontare é costituito dalla scelta della strategia più idonea e profittevole per l'utilizzo delle soluzioni cloud e per la definizione del loro corrispettivo piano di sviluppo, all'interno della quotidiana operatività dell'impresa. Per arrivare a ciò, però, occorre procedere, precedentemente, nell'analisi della situazione aziendale in merito alle capacità inerenti il cloud computing già presenti.

Nello specifico si tratta di analizzare l'esperienza aziendale in termini di:

- numero di occasioni in cui l'impresa ha affidato in "outsourcing" parte o il totale dei propri servizi legati all'information technology e i risultati e le considerazioni derivanti dall'aver fatto questo tipo di scelte.

- esperienza aziendale effettiva nell'utilizzo di strutture virtuali in ambito IT e flessibilità delle stesse ad un eventuale cambiamento in ottica cloud.

- maturità ed esperienza in termini di Service-Oriented Architecture (SOA); tanto più l'impresa annovera maturità in questo ambito, tanto più sarà lineare la transizione all'utilizzo di servizi cloud.

Verificati questi aspetti, é il momento di delineare una strategia chiara da adottare e esaustiva nel comprendere tutti gli elementi che é essenziale contenga.

Deve essere, cioé, in grado di indicare i problemi di business aziendali che l'approccio cloud sarà destinato a risolvere, spiegare come le soluzioni cloud agiranno per porre fine a questo tipo di “grattacapi” e sfide tecnologiche, illustrare quale tipo di azioni e iniziative specifiche verranno intraprese per consentire al cloud computing di raggiungere questi obiettivi e, per finire, stabilire entro quali scadenze temporali tutto questo avverrà.

Quindi, dopo avere stabilito questi fondamentali criteri sul percorso da seguire, si deve procedere alla preparazione alla fase di transizione vera e propria, che ha il suo inizio con il rendere partecipe l'intera forza lavoro del cambiamento in atto. L'organizzazione, infatti, per agevolare una più facile metabolizzazione del procedimento, deve premurarsi di rendere noto ai lavoratori il cambiamento strategico che si é deciso di attuare, come si intende procedere per l'ottenimento dello stesso e quali differenze nelle mansioni e nelle responsabilità si delineeranno.

Non solo. Fondamentale sarà istituire corsi “ad hoc”, con il fine di dotare i manager delle conoscenze e delle abilità richieste per poter operare al meglio in un contesto cloud; qualità, queste, indispensabili per poter sfruttare, in maniera più che proficua, le peculiarità dei nuovi metodi operativi a disposizione.

3.2.2 La fase della scelta del provider e del tipo di cloud

Arrivati a questo punto, basandosi sulla strategia e il processo di attuazione della stessa che sono stati precedentemente descritti, occorrerà, innanzitutto, analizzare quale sia il provider più adatto da prendere in considerazione per servirsi delle piattaforme cloud e, susseguentemente, scegliere la forma più idonea che si desidera che queste ultime abbiano[16].

3.2.3 La fase del testing

Una volta giunti alla scelta del provider, un modo intelligente di procedere, da parte dell'organizzazione, é sicuramente quello di iniziare la fase del “testing”.

La fase del testing é costituita dall'attuazione di un “progetto pilota” che consente di mettere alla prova il sistema cloud all'interno dell'azienda, raggiungendone il 60/70% della piena effettiva operatività. Questo modo di procedere, che segue una dettagliata fase di ricerca e pianificazione affinché non vi siano dubbi sulla sua reale attendibilità, é di fondamentale importanza, in quanto consente di valutare per la prima volta, dal punto di vista empirico, la concreta attuabilità del progetto.

Durante la sua esecuzione, inoltre, se si manifestassero problemi o imprevisti, si potrebbe ricorrere alla loro risoluzione più facilmente e senza rischi, al contrario di una situazione di progetto funzionante realmente e a pieno regime; la dimensione che

16 Vedi Capitolo 1, pag. 23.

lo caratterizza, infatti, ne consente un'agevole maneggiabilità e il suo status di “test” azzera i rischi di potenziali inefficienze.

3.2.4 La fase dell'azione concreta

Provveduto al compimento di tutte le fasi preliminari, é ora il momento di arrivare all'azione vera e propria. Azione che ha inizio con la stipula del contratto con il provider[17], in cui sono specificati gli oneri che il fornitore di servizi é tenuto a rispettare, le sue responsabilità e gli altri aspetti rilevanti riguardanti la fornitura del servizio. A questo punto, l'impresa é finalmente pronta per realizzare il proprio percorso strategico all'interno di un sistema di servizi cloud; tale sistema ne agevolerà l'operatività e, se pianificato efficacemente, ne migliorerà la performance.

17 Vedi Capitolo 4, pag. 78.

3.3 L'incidenza sulle risorse umane

Se, come già riferito in precedenza, l'adozione di soluzioni cloud permette all'azienda, tra le altre cose, di trovarsi a disporre di forza lavoro improvvisamente inattiva e beneficiarne reindirizzandola a rinforzare altri settori strategici[18] (senza, quindi, alcun costo aggiuntivo), va considerata anche la possibile evoluzione negativa della situazione.

Non tutti i dipendenti che, dopo l'adozione del cloud computing da parte del proprio datore di lavoro, si troveranno ad esercitare una mansione non più necessaria, infatti, avranno la fortuna di ricevere nuovi compiti da eseguire e rinnovati obiettivi da raggiungere.

Per tanti, l'avvento del cloud computing significherà l'automazione (o l'affidamento a terzi) di operazioni prima svolte internamente e la conseguente perdita del posto di lavoro; questo effetto indesiderato é forse il più preoccupante da considerare all'interno di una realtà di crescita e diffusione esponenziale di questa nuova e vantaggiosa tecnologia. (-Peter Ross, *"How to keep your head above the clouds: changing ICT worker skill sets in a cloud computing environment"*, Employment Relations Record, 2011-) (-Ching Wen Yeh, *"Cloud computing and human resources in the knowledge era"*, Human Systems Management, 2012-)

18 Vedi Capitolo 2, pag. 47.

3.4 Alcuni esempi pratici di adozione di piattaforme cloud

Esistono numerosi esempi pratici di settori in cui il diffondersi di meccanismi tipici del cloud computing ha portato a benefici evidenti e tangibili: uno di questi é certamente quello della salute.

Il fatto che il cloud computing permetta di disporre di dati in tempo reale, sia una soluzione facile da usare, sicura e accessibile da ogni luogo (con ogni dispositivo avente una connessione internet) e che sia un sistema affidabile ed economico, ha consentito al sistema sanitario di migliorare il proprio modo di operare, portando un beneficio diretto ai propri pazienti. Con un'applicazione specifica per il ramo della salute, basata su tecnologie cloud, i dati vengono, infatti, inseriti on-line con notevole facilità e ciò che viene riportato può essere istantaneamente integrato all'interno dell'intera piattaforma sanitaria, generando indicazioni e implicazioni immediate tramite appositi “rapporti”.

Questi rapporti sono di facile accesso per l'intero insieme di soggetti autorizzati, che possono procedere ad un'istantanea consultazione, indipendentemente dalla località e nazione in cui si trovino.

Grazie al cloud computing é, quindi, possibile che più ospedali condividano e aggiornino dati (e i rapporti conseguenti) in tempo reale, procedendo così alla diffusione di idee in merito, ad esempio, a cure innovative da adottare e, più in generale, a comportamenti idonei da mettere in atto a seconda della specificità dei casi dei pazienti con cui si viene a contatto. Il confronto che deriva da questo insieme

di informazioni condivise, porterà a scelte operative efficaci e, dunque, sfocerà in un generale miglioramento del sistema sanitario.

Un esempio di ciò che é appena stato illustrato può essere il dipartimento di anestesia del “California Riverside County Regional Medical Center (RCRMC)”, che fa uso di un sistema di misura interno, operante attraverso “Google Docs”, finalizzato al miglioramento continuo delle prestazioni ospedaliere.

Al RCRMC il flusso di informazioni, inserito nel database, inizia da coloro che effettuano l'anestesia e continua con le infermiere addette alla gestione del processo post-anestetico del paziente. I dati inseriti fanno riferimento al processo anestetico e ai sintomi del paziente al risveglio; in entrambi i casi, tali informazioni permettono di mettere in risalto la riuscita o meno delle diverse fasi, la qualità raggiunta nel loro svolgimento, eventuali contrattempi o risvolti negativi e la possibilità di effettuare cambiamenti a fini migliorativi.

Il tipo di dati, immessi nel sistema sottoforma di un semplice questionario da compilare all'interno della piattaforma di “Google Docs”, concorrono, istantaneamente, a formare un foglio elettronico, all'interno del quale può essere redatto facilmente un rapporto finale sulla performance. Questo insieme di rapporti, stilato quotidianamente, consente di giungere ad un'analisi periodica delle prestazioni eseguite da ogni gruppo di dottori ed infermieri operanti nell'ambito delle anestesie, potendo metterne in risalto le rispettive aree di buon operato e quelle in cui vengono rilevate delle carenze.

I vantaggi che una struttura come l' RCRMC ha potuto riscontrare nell'utilizzo di una

piattaforma cloud come “Google Docs” sono innumerevoli; tra essi i più importanti sono certamente la maneggiabilità, che consente una facile ed immediata immissione dei dati, il basso costo derivante dal suo utilizzo ed infine la possibilità di analizzare in tempo reale le varie performance svolte.

Nonostante l'iniziale scetticismo con cui questo nuovo modo di operare é stato accolto dai vari dottori/infermieri (lo si vedeva come una misura esclusivamente a scopo punitivo), susseguentemente tutti si sono accorti dei benefici che questo strumento può portare in termini di miglioramento delle tecniche da adottare per la miglior salvaguardia della salute del paziente.

Da quel momento, l'accettazione é divenuta generale e l'RCRMC ha potuto disporre di un'arma in più al servizio della buona riuscita (e dei continui progressi) del proprio operato. (-Nathan Waxer, David Ninan, Alfred Ma, Norma Dominguez, *“Continuous quality monitoring through analytics and cloud computing”*, Physician Executive, 2013-) (-Nathan Waxer, David Ninan, Alfred Ma, Norma Dominguez, *“How cloud computing and social media are changing the face of health care”*, Physician Executive, 2013-)

Un altro settore a cui il cloud computing si sta, passo dopo passo, affacciando é quello automobilistico; esempi di applicazioni inserite all'interno delle automobili, che si servono di una connessione internet wireless tramite cui accedere alle piattaforme cloud e ai rispettivi servizi, sono sicuramente “MyRate” (che ha rappresentato il pioniere per le applicazioni cloud in ambito automobilistico e che permette alle compagnie di assicurazioni di immagazzinare dati riguardanti la guida

di un potenziale cliente e deciderne, conseguentemente, il premio assicurativo più consono da applicare al momento della definizione dell'accordo) e “MyFord Mobile”. Quest'ultima, specificatamente pensata per il modello elettrico commercializzato da “Ford”, consente di avere accesso, in tempo reale, ad una serie di informazioni stradali (ad esempio i luoghi di interesse nelle vicinanze) o connesse alle prestazioni (come ad esempio la velocità media del tragitto in corso), ma soprattutto aiuta a gestire al meglio la quantità di batteria rimasta a disposizione, indicando se il viaggio pianificato possa risultare eccessivamente lungo per la capacità energetica che si possiede. (-Dimitar Filev, Jianbo Lu, Davor Hrovat, *“Future mobility: integrating vehicle control with cloud computing”*, Mechanical Engineering, 2013-)

Capitolo 4

IL CONTRATTO TRA PROVIDER E CLIENTE E LA PROBLEMATICA DELLA SICUREZZA

4.1 La stipula del contratto

Il momento della stipula del contratto é una fase fondamentale per il raggiungimento, da parte dell'azienda, dei benefici insiti nel mondo cloud.

In quanto fase fondamentale, perciò, va definità e curata con la dovuta attenzione, visto che da essa dipenderanno molti dei destini legati al rapporto con il provider.

Il primo passo che l'organizzazione deve avere in mente di affrontare, é quello di procedere con cura all'analisi di tutti gli elementi che caratterizzeranno il contratto di fornitura di servizi proposto dai diversi cloud provider disponibili sul mercato, arrivando a scegliere quello più in linea con le proprie aspettative e necessità.

Nel caso, poi, in cui l'impresa si trovi in una situazione di elevata forza contrattuale,

sarà, a quel punto, conveniente che si tuteli contro le future eventuali variazioni del contratto stesso, decise dal provider. Come? Provvedendo all'inserimento di alcune clausole contrattuali: tali clausole dovrebbero specificare che ogni futuro cambiamento dei servizi offerti dal provider non dovrà, in alcun modo, intaccare il livello della performance e della protezione dei dati offerti da quest'ultimo alla data di sottoscrizione del contratto e non dovrà imporre alcun nuovo obbligo nei confronti dell'impresa. (-James R. Kalyvas, Michael R. Overly, Matthew A. Karlyn, *"Cloud computing: a practical framework for managing cloud computing risk"*, Intellectual property & technology law journal, 2013-)

A dover di cronaca, però, é corretto sottolineare che, nella stragrande maggioranza dei casi, l'impresa che decide di adottare soluzioni cloud, si limiterà a considerare i vari "Terms & Conditions" alla base dei contratti dei vari provider e ad optare per quello più conforme alle sue esigenze. E' parecchio raro, come vedremo qui di seguito, che l'organizzazione abbia un potere tale da poter pretendere ed ottenere un cambiamento esclusivo delle condizioni contrattuali, predeterminate per l'intero bacino di clientela, offerte dai vari fornitori di servizi cloud.

Inizieremo, ora, una rassegna dettagliata dei già citati "Terms & Conditions" che l'impresa necessita di analizzare, con estrema attenzione, prima di procedere alla sottoscrizione del contratto con uno degli svariati cloud provider presi in considerazione; nello specifico faremo riferimento ai termini commerciali e legali caratterizzanti la collaborazione provider/cliente ["Terms of Services" (ToS)], agli

accordi relativi al livello di performance desiderato nella fornitura del servizio e alle conseguenti misure di compensazione eventualmente offerte nel caso in cui tale livello non venisse raggiunto ["Service-Level Agreements" (SLA)] e all'approccio del provider nell'uso e nella protezione dei dati "fornitigli" in gestione dal cliente ("Privacy Policies"):

- *Legge vigente:* devono essere stabilite con esattezza l'insieme di leggi, facenti capo ad una specifica giurisdizione, a cui il contratto intende uniformarsi. Solitamente si fa riferimento alla giurisdizione nella quale il provider ha la sua sede di business principale, ma in alcuni casi si specifica che, in base al luogo di provenienza del consumatore del servizio, saranno in vigore diversi obblighi legislativi.

- *Risoluzione legale dei conflitti:* generalmente, al fine di evitare problemi di compatibilità, per risolvere le eventuali dispute che potranno sorgere tra provider e consumatore, viene indicata la medesima giurisdizione scelta per la definizione del sistema legislativo a cui sottostare.

- *Arbitraggio:* il contratto di cloud computing, come molti altri contratti di tipo commerciale, può stabilire la possibilità di ricorrere ad un collegio arbitrale per la risoluzione dei conflitti tra provider e consumatore.

- *Uso consentito del servizio offerto:* é compito del provider premurarsi di indicare con precisione l'uso che il consumatore é tenuto a fare dei servizi che egli offre. Nel dettaglio, il cloud provider declina la propria responsabilità e si riserva la possibilità di recedere dai suoi obblighi contrattuali, se la condotta non esemplare del cliente lo spinge a compiere un insieme di azioni (che spesso vengono elencate meticolosamente nel contratto) dirette ad un uso illegale o improprio del servizio offerto (esempi possono essere gioco d'azzardo, frode, “hackeraggio”, immissione di materiale pornografico, ecc...). In aggiunta, il provider si prodiga nello specificare il divieto di utilizzo dei contenuti all'interno dei propri servizi da parte del cliente (nei casi in cui tale utilizzo non rientri nel previsto contratto di collaborazione), se non in presenza di una sua autorizzazione; all'interno di questo tipo di divieto rientra, ovviamente, anche l'uso del proprio marchio/logo di rappresentanza.

- *Proprietà dei dati e diritti di utilizzo:* é fondamentale la presenza dell'indicazione esplicita che, anche in seguito al trasferimento dei dati dell'organizzazione all'interno delle strutture cloud del provider, il diritto di proprietà su di essi rimarrà sempre esclusivamente in mano all'impresa (ciò permette di evitare dispute nel caso il provider terminasse di fornire i propri servizi e il cliente chiedesse la restituzione dei propri dati da esso posseduti). Non solo. Considerato il fatto che il provider avrà accesso a questi dati per l'intera durata dell'accordo della fornitura dei servizi cloud, é fortemente

consigliabile di verificare l'esistenza di clausole contrattuali che specifichino l'obbligo di tale soggetto di mantenere le informazioni a livello confidenziale e limitarne l'effettivo uso che questi é autorizzato a farne (nel dettaglio, é consigliato di controllare che sia presente l'indicazione che il provider potrà servirsi dei dati del cliente, perlomeno di quelli “sensibili”, solo in ottemperanza allo svolgimento delle mansioni a cui é preposto, che sono indicate nel contratto stesso).

- *Rilascio a terzi di dati di proprietà del cliente:* al di là di ogni tipo di indicazione del provider nel contratto, riguardante la salvaguardia del carattere confidenziale dei dati del cliente, vi sono alcuni casi in cui si presentano delle eccezioni al riguardo. Con più o meno grande accuratezza, infatti, i vari provider sottolineano, all'interno dell'accordo, il loro obbligo a rilasciare qualsiasi genere di informazione in loro possesso, in situazioni particolari di tipo legale (quale, ad esempio, un'esplicita richiesta da parte della corte giudiziaria) o riguardanti il pubblico interesse; questo rilascio di informazioni, però, viene, secondo una prassi comunemente adottata, preceduto da un avviso dal provider al cliente.

- *Responsabilità del provider nella fornitura dei servizi:* é compito del provider attenersi alle indicazioni, da egli stesso fornite, nel contratto a cui, in principio, il consumatore ha aderito e, quindi, assicurare, per l'intera durata del rapporto, un servizio puntuale e soprattutto in linea con gli standard predeterminati.

- *Responsabilità del provider per danni economici nell'uso dei suoi servizi:* il provider si dichiara, nella quasi totalità dei casi, non responsabile di eventuali danni economici, di ogni sorta, occorsi al cliente nell'utilizzo dei propri servizi; "in ogni caso", per ciò che riguarda i danni ragionevolmente prevedibili e "secondo le norme di legge", in tutti gli altri casi.

- *Responsabilità del provider in termini di integrità dei dati di proprietà del cliente:* la maggior parte dei provider, pur dotandosi di sistemi di protezione dei dati all'avanguardia, tra i migliori sul mercato e continuamente aggiornati, ci tiene ad indicare esplicitamente nel contratto di non essere responsabile per alcun accesso non autorizzato degli stessi proveniente dall'esterno.

  In poche parole, ogni fornitore di servizi cloud si impegna a fare il massimo perché ciò non avvenga, anche per i negativi risvolti di immagine a cui, in tal caso, si esporrebbe, ma non vuole alcuna responsabilità legale se ciò si venisse malauguratamente e inaspettatamente a verificare. (-Simon Bradshaw, Christopher Millard, Ian Walden, *"Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services"*, International Journal of Law and Information Technology, 2011-)

- *Indennizzo a favore del cliente:* sebbene la maggior parte dei provider faccia il possibile per limitare la propria responsabilità nel caso di elementi, non sotto il loro diretto controllo, che concorrano al fallimento della fornitura del servizio secondo gli standard predeterminati, il discorso cambia nella situazione in cui

l'inefficienza sia a loro imputabile.

A fronte di un caso simile (i vari elementi che portano a questo tipo di casistica vengono illustrati scrupolosamente nel contratto), la quasi totalità di essi offre un compenso (quasi sempre sottoforma di crediti per l'utilizzo del medesimo servizio in futuro) per rimediare al mancato rispetto degli accordi presi.

- *Indennizzo a favore del provider:* molto spesso il provider si mette al riparo da eventuali comportamenti impropri o illegali da parte del cliente, nell'utilizzo dei suoi servizi, procedendo all'inserimento di specifiche indicazioni all'interno del contratto, dalle quali scaturisca l'obbligo di un indennizzo (e il suo corrispettivo ammontare) a seconda del caso di vietata/cattiva condotta riscontrato.

- *Garanzie:* esiste uno svariato numero di garanzie di cui l'impresa, che si avvicina ai servizi cloud, dovrebbe controllare l'esistenza all'interno del contratto del provider a cui aderisce.

  Di seguito se ne elencano alcuni esempi:

✔ I servizi forniti dal provider devono attenersi alle leggi e alle regolamentazioni nazionali, regionali e locali.

✔ I servizi offerti non devono infrangere alcun diritto di proprietà intellettuale di qualsiasi terza parte.

- ✔ I servizi offerti non devono contenere virus o altri programmi potenzialmente dannosi.

- ✔ Il provider si premurerà di offrire attività di consulenza per l'utilizzo dei propri servizi da parte del cliente, qualora richiesto.

- ✔ In linea con gli accordi presi, il provider deve fornire il proprio servizio in maniera professionale e puntuale utilizzando personale qualificato.

  La realtà, però, é che raramente il provider fornirà specifiche garanzie di questo genere al cliente che si appresta ad usufruire dei suoi servizi; assicurerà il suo massimo impegno nel fare in modo che il servizio offerto sia il migliore e il più sicuro possibile, ma di rado si spingerà oltre arrivando ad autoimporsi un dettagliato modo di operare o a pubblicare vere e proprie “promesse” di rendimento.

- *Variazione dei termini contrattuali:* la variazione dei termini contrattuali dipende, tipicamente, dall'indicazione che ne viene fatta nel contratto originario. In taluni casi tale modifica può avvenire solo con consenso scritto sia del provider che del consumatore, in altri, invece, il provider provvede alla modifica dei “termini” e delle “condizioni” del contratto e ne carica la nuova versione sul proprio sito web (solamente alcuni fornitori di servizi avvisano il cliente, via e-mail, dell'avvenuto cambiamento); a quel punto, in caso di servizio a pagamento, il cliente potrà recedere entro un determinato termine

prestabilito oppure continuare ad usufruire dei “servigi” del provider “annunciando”, così, la tacita accettazione della nuova forma contrattuale.

- *Termine del servizio da parte del consumatore:* per ciò che concerne il termine del servizio da parte del consumatore vanno fatte due distinzioni principali.

  Nel caso in cui il consumatore non stia pagando il servizio di cui usufruisce, egli potrà recedere dallo stesso in qualsiasi momento.

  Se, invece, vi é un pagamento della prestazione e, quindi, un contratto in cui vi é indicata esplicitamente una data di fine della collaborazione, bisogna rifarsi alle norme diffuse dal provider e accettate dal consumatore al momento della sottoscrizione del contratto stesso. Importante sottolineare che, di norma, il consumatore che decidesse di interrompere il servizio prima del termine, sarà, comunque, obbligato al pagamento dei servizi per l'intera durata dell'accordo. In caso di “default” del provider, però, generalmente il cliente ha la possibilità di recedere dall'accordo per il mancato rispetto dello stesso (e di ottenere, ove previsto, un indennizzo per il danno subito).

- *Termine del servizio da parte del provider:* anche per ciò che riguarda il termine del servizio da parte del provider vanno fatte due distinzioni principali.

  Nel caso in cui il consumatore non stia pagando il servizio di cui usufruisce, il provider potrà recedere dalla fornitura dello stesso in qualsiasi momento (con o senza preavviso a seconda dei casi).

  Se, invece, vi é un pagamento della prestazione e, quindi, un contratto in cui vi

é indicata esplicitamente una data di fine della collaborazione, bisogna rifarsi alle norme diffuse dal provider e accettate dal consumatore al momento della sottoscrizione del contratto stesso.

Solitamente il provider può interrompere l'accordo se non riceve il pagamento della prestazione entro i termini pattuiti o se il cliente adotta una condotta illegale o non in linea con le norme imposte dal contratto (o utilizza contenuti dello stesso genere).

- *Preservazione/cancellazione dei dati al termine della collaborazione:* la preservazione dei dati, in seguito alla conclusione della collaborazione con il provider, é di fondamentale importanza per il cliente; quest'ultimo, infatti, deve avere la certezza che essi non vadano persi, per poter procedere al loro recupero e farne di nuovo uso all'interno dell'azienda.

  Allo stesso tempo é importante che sia presente, all'interno del contratto, la promessa di cancellazione degli stessi dalle piattaforme cloud dopo l'avvenuto recupero; il cliente deve avere la certezza, infatti, che tali informazioni non siano più a disposizione dell'ex fornitore del servizio che, altrimenti, potrebbe farne un uso improprio/non consentito.

  A testimonianza di tutto ciò, la maggior parte dei provider stabilisce, nei dettami del contratto, che preserverà l'intero ammontare dei dati dei clienti per circa un mese prima di procedere alla totale cancellazione degli stessi.

- *Proprietà del data center:* se il provider é il proprietario del software di cui il cliente fa utilizzo, ma non il possessore del data center in cui il software stesso opera, é bene che il cliente si assicuri che nel contratto siano presenti alcuni obblighi a cui esso é tenuto:

✔ assicurarsi che la terza parte in gioco rispetti gli obblighi contrattuali definiti tra esso e il proprio cliente, inclusi quelli riguardanti la sicurezza dei dati.

✔ accettare la responsabilità diretta per tutte le azioni compiute dalla terza parte.

✔ provvedere a rimediare immediatamente ad eventuali comportamenti, da parte della terza parte, non in linea con i dettami contrattuali.

- *Disaster recovery e continuità di business:* sarebbe di rilevante importanza che fosse presente, all'interno del contratto, la promessa del provider e la conseguente dimostrazione effettiva (tramite presentazione del "disaster recovery plan" e dell'ultimo test effettuato per verificarne il funzionamento), di essere in grado di garantire la continuità del servizio e la protezione dei dati, anche in caso di anomalie di funzionamento impreviste (nel caso di dilungati malfunzionamenti, il provider vi pone rimedio, solitamente, ricorrendo ad un server/data center secondario o, qualora ciò non sia possibile, usufruendo di un altro provider).

  L'esistenza di questo tipo di requisito andrebbe a fornire adeguata assicurazione contrattuale che i servizi verranno erogati per l'intera durata

dell'accordo. (-Joshua Gold, *"Protection in the cloud: risk management and insurance for cloud computing"*, Journal of internet law, 2012-)

- *Reputazione della controparte:* é conveniente, per entrambe le parti in gioco, accertarsi che all'interno del contratto siano previste alcune limitazioni imposte nel rispetto dell'altrui immagine.

  Per questo motivo dovrebbe essere esplicitato il divieto di utilizzo del nome o del marchio della controparte e della possibilità di fornire annunci pubblici relativi all'accordo raggiunto, a meno che non vi sia stata una precedente autorizzazione scritta che lo consenta.

- *Negoziazione preventiva di eventuali "tasse" addizionali:* é bene assicurarsi preventivamente sull'eventuale esistenza di quote aggiuntive da pagare in caso di variazioni del servizio. Il provider potrebbe, infatti, decidere di applicare un sovrapprezzo in caso di superamento di una certa quota di immagazzinamento dati o di necessità di nuovi aggiornamenti di software; a quel punto l'impresa in questione dovrebbe prodigarsi nel verificare che tali azioni trovino riscontro e giustificazione nel contratto firmato in origine dai contraenti.

- *Back up dei dati:* é importante che l'impresa verifichi che il provider, all'interno del contratto, abbia possibilmente specificato, tra i suoi doveri, di procedere ad un frequente back up[19] dei dati del cliente e alla diffusione delle relative

19 "*Back up" dei dati:* si parla di back up dei dati (o copia di sicurezza), per riferirsi alla replicazione, su un qualunque supporto di memorizzazione, di materiale informativo archiviato nella memoria di massa dei computer, al fine di prevenire la perdita dei dati in caso di eventi malevoli accidentali o intenzionali.

comunicazioni informative che ne testimoniano la riuscita effettiva. Si tratterebbe di un requisito non trascurabile e potenzialmente discriminante nella scelta del fornitore di servizi cloud.

- *Bancarotta del provider:* normalmente, all'interno del contratto, viene stabilito che, nella circostanza di bancarotta del provider, il cliente abbia il diritto di terminare "in seduta stante" la validità dell'accordo.

  Nell'eventualità in cui l'impresa nutra fin dal principio delle perplessità sulla stabilità finanziaria del provider, sarà sua premura cercare di ottenere, nell'accordo scritto, l'aggiunta di clausole che obblighino quest'ultimo a redigere e consegnare periodici "report" sull'andamento delle proprie finanze. Così facendo l'impresa avrà a disposizione i dati necessari per poter prevedere, in anticipo, se il provider possa avere problemi nel rispetto degli accordi iniziali e, se così fosse, agire di conseguenza con il fine di ridurre al minimo gli impatti negativi derivanti dal realizzarsi di tale eventualità.

Nella tabella qui di seguito forniremo un confronto, a titolo di esempio, delle caratteristiche degli elementi principali, tra quelli sopra citati, riscontrabili nei T&C di ogni specifico contratto sottoscritto da 10 tra i cloud provider più rinomati a livello internazionale al giorno d'oggi: Akamai, Amazon, Apple, Dropbox, Facebook, Google, IBM, Microsoft, Rackspace e Salesforce.com.

La rappresentazione ci sarà utile anche per le considerazioni sulla sicurezza che scaturiranno nel paragrafo seguente;

CLOUD PROVIDER T&C	AKAMAI	AMAZON	APPLE	DROPBOX
TIPO DI SERVIZIO OFFERTO	IaaS	SaaS, IaaS	SaaS	SaaS
LEGGE VIGENTE	Massachusetts State (USA)	Washington State (USA)	California State (USA)	California State (USA)
UTILIZZO CONSENTITO DEL SERVIZIO OFFERTO	-Secondo legge e secondo le condizioni definite da Akamai (indicate dettagliatamente nella "Acceptable Use Policy"). -Akamai declina ogni responsabilità per comportamenti del cliente contro la legge o non in linea con i termini previsti nel contratto e per l'immissione di contenuti illegali o offensivi.	-Secondo legge e secondo le condizioni definite da Amazon. -Nessuna responsabilità su condotta e contenuti, immessi dal cliente, di tipo illegale o offensivo, e riguardo ad altri comportamenti specificati esplicitamente nell' "Acceptable Use Policy" di Amazon. In questi casi, Amazon può decidere per la sospensione o l'eliminazione del cliente dalle proprie piattaforme cloud.	-Secondo legge e secondo le condizioni definite da Apple. -Apple declina ogni responsabilità per comportamenti del cliente contro la legge o non in linea con i termini previsti nel contratto (i casi di cattiva condotta che il cliente non deve adottare sono indicati nel dettaglio nel T&C di Apple) e per l'immissione di contenuti illegali o offensivi.	-Secondo legge e secondo le condizioni definite da Dropbox. -Dropbox declina ogni responsabilità per comportamenti del cliente contro la legge o non in linea con i termini previsti nel contratto e per l'immissione di contenuti illegali o offensivi.
PROPRIETA' DATI	Cliente	Cliente	Cliente	Cliente
DIRITTI DI UTILIZZO DATI DEL CLIENTE	-Akamai non condivide alcun dato di proprietà dei propri clienti con terzi, se non dopo loro esplicita autorizzazione. -Casi particolari: se richiesti dalla legge o in caso di altre ragioni di pubblico interesse, il provider diffonderà i dati in ogni caso.	-Amazon non è autorizzata all'utilizzo dei dati forniti dal cliente, se non per lo scopo per cui essi sono stati resi disponibili sulle sue piattaforme (a meno che vi sia un'autorizzazione da parte del cliente). -Casi particolari: il provider fornirà i dati del cliente a terzi, solo nel caso siano espressamente richiesti dalla legge.	-Apple non è autorizzata all'utilizzo dei dati forniti dal cliente, se non per lo scopo per cui essi sono stati resi disponibili sulle sue piattaforme (a meno che vi sia un'autorizzazione da parte del cliente). -Casi particolari: il provider fornirà i dati del cliente a terzi, solo nel caso siano espressamente richiesti dalla legge o per salvaguardare la sicurezza e l'immagine sua e/o quella della propria clientela.	-Dropbox non condivide alcun dato di proprietà dei propri clienti con terzi, se non dopo loro esplicita autorizzazione. -Casi particolari: il provider fornirà i dati del cliente a terzi, solo nel caso siano espressamente richiesti dalla legge o per salvaguardare la sicurezza e l'immagine sua e/o quella della propria clientela.
RESPONSABILITA' PROVIDER PER FORNITURA SERVIZI	Akamai si impegna ad offrire i servizi richiesti come indicato all'interno del contratto.	Nessuna. Amazon si impegna ad offrire i servizi richiesti come indicato da contratto, ma il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricade interamente sul cliente.	Nessuna. Apple si impegna ad offrire i servizi richiesti come indicato da contratto, ma il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricade interamente sul cliente.	Nessuna. Dropbox si impegna ad offrire i servizi richiesti come indicato da contratto, ma il rischio legato all'effettiva fornitura dei servizi richiesti e al loro contenuto ricade interamente sul cliente.

FACEBOOK	GOOGLE	IBM	MICROSOFT	RACKSPACE	SALESFORCE.COM
SaaS	SaaS, PaaS	IaaS	SaaS, PaaS, IaaS	IaaS	SaaS
California State (USA)	California State (USA)	Non specificato.	Dipende dalla nazione in cui si trova il cliente.	Dipende dalla nazione in cui si trova il cliente.	Dipende dalla nazione in cui si trova il cliente.
Secondo legge e secondo le norme indicate nella "Dichiarazione dei diritti e delle responsabilità" pubblicata da Facebook (alla voce "sicurezza" sono specificati i comportamenti che il cliente non deve tenere).	-Secondo legge e secondo le condizioni definite da Google. -Google declina ogni responsabilità per comportamenti del cliente contro la legge o non in linea con i termini previsti nel contratto e per l'immissione di contenuti illegali o offensivi.	-Secondo legge e secondo le condizioni definite da IBM. -IBM declina ogni responsabilità per comportamenti del cliente contro la legge o non in linea con i termini previsti nel contratto e per l'immissione di contenuti illegali o offensivi.	Secondo legge e secondo le condizioni definite da Microsoft (per una rassegna dettagliata dei comportamenti consentiti, consultare "Microsoft Anti-Spam Policy" e "Microsoft Code of Conduct").	Secondo legge e secondo le condizioni definite da Rackspace (per una rassegna dettagliata dei comportamenti consentiti, consultare l' "Acceptable Use Policy").	Secondo legge e secondo le condizioni definite da Salesforce.com (per una rassegna dettagliata dei comportamenti consentiti, consultare il "Master Subscription Agreement").
Cliente	Cliente	Cliente	Cliente	Cliente	Cliente
L'utente, una volta pubblicato del contenuto all'interno del proprio profilo Facebook, concede una licenza non esclusiva, trasferibile, nell'utilizzo, a discrezione del provider, dello stesso. Tale utilizzo terminerà solo qualora l'utente elimini il suo account (o i contenuti al suo interno), a meno che tali contenuti non siano stati condivisi con terzi e che questi non li abbiano eliminati a loro volta. Oltretutto è possibile che i contenuti rimossi vengano conservati come copie di back-up per circa 90 giorni (pur non essendo visibili ad altri se non al provider).	-Google si riserva il diritto di usufruire dei dati del cliente a suo piacimento per ciò che concerne l'utilizzo, la promozione, il miglioramento e lo sviluppo dei propri servizi (secondo i principi indicati nelle "norme sulla privacy"). -Casi particolari: il provider fornirà i dati del cliente a terzi, solo nel caso siano espressamente richiesti dalla legge o per salvaguardare la sicurezza e l'immagine sua e/o quella della propria clientela.	-IBM non è autorizzata all'utilizzo dei dati forniti dal cliente, se non per lo scopo per cui essi sono stati resi disponibili sulle sue piattaforme (a meno che vi sia un'autorizzazione da parte del cliente). -Casi particolari: il provider fornirà i dati del cliente a terzi, solo nel caso siano espressamente richiesti dalla legge o per salvaguardare la sicurezza e l'immagine sua e/o quella della propria clientela.	-Microsoft si riserva il diritto di usufruire dei dati del cliente a suo piacimento, per ciò che concerne l'utilizzo, la promozione, il miglioramento e lo sviluppo dei propri servizi e le operazioni necessarie per proteggere il cliente stesso. -Casi particolari: il provider fornirà i dati del cliente a terzi, solo nel caso siano espressamente richiesti dalla legge o per salvaguardare la sicurezza e l'immagine sua e/o quella della propria clientela.	-Rackspace non condivide alcun dato di proprietà dei propri clienti con terzi, se non dopo loro esplicita autorizzazione. -Casi particolari: Rackspace fornirà i dati del cliente a terzi, solo nel caso siano espressamente richiesti dalla legge o siano necessari per salvaguardare la sicurezza e l'immagine sua e/o quella della propria clientela (avvisando preventivamente il cliente stesso).	-Salesforce.com non condivide alcun dato di proprietà dei propri clienti con terzi, se non dopo loro esplicita autorizzazione. -Casi particolari: Salesforce.com fornirà i dati del cliente a terzi, solo nel caso siano espressamente richiesti dalla legge o siano necessari per portare a termine l'offerta del servizio/prevenire problemi tecnici allo stesso (in ogni caso, però, provvederà ad informare preventivamente il cliente).
Nessuna. Facebook si impegna ad offrire i servizi richiesti come indicato da contratto, ma il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricade interamente sul cliente.	Nessuna. Google si impegna ad offrire i servizi richiesti come indicato da contratto, ma il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricade interamente sul cliente.	Nessuna. IBM si impegna ad offrire i servizi richiesti come indicato da contratto, ma il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricade interamente sul cliente.	-Microsoft è responsabile per il mancato rispetto degli accordi del contratto, solo nel caso esso sia imputabile a suoi atti di negligenza. -Va specificato, però, che se Microsoft dovesse interrompere la fornitura del servizio al cliente senza "giusta causa", sarà suo dovere provvedere al rimborso allo stesso della parte di servizio pagata, ma, poi, non fornita.	Rackspace è responsabile per l'effettiva fornitura dei suoi servizi; in caso di eventuali problemi, provvederà ad indennizzare il cliente tramite rimborso delle quote versate.	Salesforce.com si impegna a garantire l'offerta dei servizi richiesti secondo i dettami indicati espressamente nel contratto di fornitura a cui il cliente ha aderito.

CLOUD PROVIDER T&C	AKAMAI	AMAZON	APPLE	DROPBOX
RESPONSABILITA' PROVIDER PER INTEGRITA' DATI DEL CLIENTE	Nessuna, ove permesso dalla legge. E in ogni caso MAI per perdite o danni ragionevolmente prevedibili. Il provider specifica che utilizzerà meccanismi all'avanguardia per preservare l'integrità dei dati, ma non ne garantisce il successo.	Nessuna, ove permesso dalla legge. E in ogni caso MAI per perdite o danni ragionevolmente prevedibili. Il provider specifica che utilizzerà meccanismi all'avanguardia per preservare l'integrità dei dati, ma non ne garantisce il successo.	Nessuna, ove permesso dalla legge. Il provider specifica che utilizzerà meccanismi all'avanguardia per preservare l'integrità dei dati, ma non ne garantisce il successo.	Nessuna, ove permesso dalla legge. E in ogni caso MAI per perdite o danni ragionevolmente prevedibili. Il provider specifica che utilizzerà meccanismi all'avanguardia per preservare l'integrità dei dati, ma non ne garantisce il successo.
INDENNIZZO A FAVORE DEL CONSUMATORE (ESCLUSIVAMENTE PER SERVIZI CLOUD A PAGAMENTO)	-Nel caso in cui il provider venga riconosciuto colpevole dalla legge di un rimborso al cliente, tale rimborso non potrà mai superare ciò che il cliente ha versato nei 6 mesi precedenti la domanda di indennizzo. -Casi particolari: in caso di ricorsi legali contro il cliente per violazioni di "diritti di proprietà intellettuale" di terzi dipendenti dai servizi offerti dal provider, il cliente deve informare tempestivamente Akamai che si curerà della sua difesa e di indennizzare ogni costo/danno subito derivante da questo tipo di procedimento. Tale copertura da parte del provider non sarà presente in caso di ricorsi avvenuti per il contenuto immesso dal cliente o se quest'ultimo non ha rispettato i termini contrattuali nell'utilizzo dei servizi.	Nel caso in cui il provider venga riconosciuto colpevole dalla legge di un rimborso al cliente, tale rimborso non potrà mai superare ciò che il cliente ha versato nei 12 mesi precedenti la domanda di indennizzo.	Nessun riferimento specifico.	Nel caso in cui il provider venga riconosciuto colpevole dalla legge di un rimborso al cliente, tale rimborso non potrà mai superare i $20 oppure ciò che il cliente ha versato nei 3 mesi precedenti la domanda di indennizzo.
INDENNIZZO A FAVORE DEL PROVIDER	Il cliente ha il dovere di rispondere ad eventuali ricorsi legali contro il provider provenienti da terzi (e procedere all'indennizzo delle eventuali spese e danni da essi provocati al provider stesso), dipendenti dalla propria condotta o dal contenuto immesso nei servizi.	Il cliente ha il dovere di rispondere ad eventuali ricorsi legali contro il provider provenienti da terzi (e procedere all'indennizzo delle eventuali spese e danni da essi provocati al provider stesso), dipendenti dalla propria condotta o dal contenuto immesso nei servizi.	Il cliente ha il dovere di rispondere ad eventuali ricorsi legali contro il provider provenienti da terzi (e procedere all'indennizzo delle eventuali spese e danni da essi provocati al provider stesso), dipendenti dalla propria condotta o dal contenuto immesso nei servizi.	Il cliente ha il dovere di rispondere ad eventuali ricorsi legali contro il provider provenienti da terzi (e procedere all'indennizzo delle eventuali spese e danni da essi provocati al provider stesso), dipendenti dalla propria condotta o dal contenuto immesso nei servizi.

FACEBOOK	GOOGLE	IBM	MICROSOFT	RACKSPACE	SALESFORCE.COM
Nessuna.	Nessuna, ove permesso dalla legge. E in ogni caso MAI per perdite o danni ragionevolmente prevedibili. Il provider specifica che utilizzerà meccanismi all'avanguardia per preservare l'integrità dei dati, ma non ne garantisce il successo.	Nessuna, ove permesso dalla legge. Il provider specifica che utilizzerà meccanismi all'avanguardia per preservare l'integrità dei dati, ma non ne garantisce il successo.	Nessuna, ove permesso dalla legge. E in ogni caso MAI per perdite o danni ragionevolmente prevedibili. Il provider specifica che utilizzerà meccanismi all'avanguardia per preservare l'integrità dei dati, ma non ne garantisce il successo.	Rackspace afferma che l'integrità dei dati verrà garantita, qualora il cliente abbia proceduto al pagamento di specifici servizi di back-up addizionali.	Nessuna, ove permesso dalla legge. E in ogni caso MAI per perdite o danni ragionevolmente prevedibili. Il provider specifica che utilizzerà meccanismi all'avanguardia per preservare l'integrità dei dati, ma non ne garantisce il successo.
Nel caso in cui il provider venga riconosciuto colpevole dalla legge di un rimborso al cliente, tale rimborso non potrà mai superare i $100.	-Nel caso in cui il provider venga riconosciuto colpevole dalla legge di un rimborso al cliente, tale rimborso non potrà mai superare ciò che il cliente ha versato per l'utilizzo del servizio. -Casi particolari: in caso di ricorsi legali contro il cliente per violazioni di "diritti di proprietà intellettuale" di terzi dipendenti dai servizi offerti dal provider, il cliente deve informare tempestivamente Google che si curerà della sua difesa e di indennizzare ogni costo/danno subito derivante da questo tipo di procedimento. Tale copertura da parte del provider non sarà presente in caso di ricorsi avvenuti per il contenuto immesso dal cliente o se quest'ultimo non ha rispettato i termini contrattuali nell'utilizzo dei servizi.	Nessun riferimento specifico.	Nel caso in cui il provider venga riconosciuto colpevole dalla legge di un rimborso al cliente, tale rimborso non potrà mai superare ciò che il cliente ha versato per l'utilizzo del servizio.	Per ogni 30 minuti di eventuale inattività, Rackspace rimborserà al cliente il 5% del totale che egli versa mensilmente per l'utilizzo dei servizi (fino a raggiungere il 100% dell'esborso, ma non oltre).	-Nel caso in cui il provider venga riconosciuto colpevole dalla legge di un rimborso al cliente, tale rimborso non potrà mai superare l'ammontare che il cliente ha versato nei 12 mesi precedenti la domanda di indennizzo. -Casi particolari: in caso di ricorsi legali contro il cliente per violazioni di "diritti di proprietà intellettuale" di terzi dipendenti dai servizi offerti dal provider, il cliente deve informare tempestivamente Salesforce.com che si curerà della sua difesa e di indennizzare ogni costo/danno subito derivante da questo tipo di procedimento. Tale copertura da parte del provider non sarà presente in caso di ricorsi avvenuti per il contenuto immesso dal cliente o se quest'ultimo non ha rispettato i termini contrattuali nell'utilizzo dei servizi.
Il cliente ha il dovere di rispondere ad eventuali ricorsi legali contro il provider provenienti da terzi (e procedere all'indennizzo delle eventuali spese e danni da essi provocati al provider stesso), dipendenti dalla propria condotta o dal contenuto immesso nei servizi.	Il cliente ha il dovere di rispondere ad eventuali ricorsi legali contro il provider provenienti da terzi (e procedere all'indennizzo delle eventuali spese e danni da essi provocati al provider stesso), dipendenti dalla propria condotta o dal contenuto immesso nei servizi.	Nessun riferimento specifico.	Il cliente ha il dovere di rispondere ad eventuali ricorsi legali contro il provider provenienti da terzi (e procedere all'indennizzo delle eventuali spese e danni da essi provocati al provider stesso), dipendenti dalla propria condotta o dal contenuto immesso nei servizi.	Nessun riferimento specifico.	Il cliente ha il dovere di rispondere ad eventuali ricorsi legali contro il provider provenienti da terzi (e procedere all'indennizzo delle eventuali spese e danni da essi provocati al provider stesso), dipendenti dalla propria condotta o dal contenuto immesso nei servizi, risultante di tipo illegale o in violazione di "diritti di proprietà intellettuale".

CLOUD PROVIDER T&C	AKAMAI	AMAZON	APPLE	DROPBOX
VARIAZIONI TERMINI CONTRATTUALI	Le variazioni agli originari termini contrattuali sono consentite e divengono effettive solamente se in forma scritta e firmate in calce sia dal provider, sia dal cliente (solo in caso di servizi cloud a pagamento).	Se vengono fatte, il provider aggiornerà i T&C sul sito web (informando, preventivamente, il cliente via e-mail in caso di servizi cloud a pagamento) e da quel momento, tali modifiche, diverranno effettive; il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.	Se vengono fatte, il provider aggiornerà i T&C sul sito web e da quel momento, tali modifiche, diverranno effettive; il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.	Se vengono fatte, il provider aggiornerà i T&C sul sito web (nei casi di "modifiche importanti" e di servizi a pagamento, informando il cliente via e-mail) e da quel momento, tali modifiche, diverranno effettive; il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.
TERMINE DEL SERVIZIO (I CASI CONSIDERATI SONO SERVIZI CLOUD A PAGAMENTO. PER I SERVIZI GRATUITI PROVIDER E CLIENTE POSSONO RECEDERE DALLA COLLABORAZIONE A DISCREZIONE PERSONALE E SENZA SOTTOSTARE AD ALCUNA CONDIZIONE)	-Ognuna delle parti può recedere se il contraente non rispetta l'accordo contrattuale e perseverà nel comportamento doloso per 30 giorni di fila (es. il provider non riceve i pagamenti dovuti entro 30 giorni dalla data prevista) -Se il cliente interrompe il contratto prima della fine dello stesso, sarà comunque tenuto a pagare l'intero servizio al provider. -Se prima di 60 giorni dalla scadenza, una delle due parti non afferma di non volere continuare il rapporto, il rinnovo dello stesso avverrà automaticamente.	-Ognuna delle due parti può decidere, a sua completa discrezione, di terminare il servizio qualora lo ritenga necessario; Amazon, però, nel caso, dovrà dare 30 giorni di preavviso (sospensione della collaborazione "per convenienza"). -Ognuna delle parti può recedere se l'altro contraente non rispetta uno o più accordi contrattuali e perseverà nel comportamento doloso per 30 giorni di fila. Amazon, in casi specifici riportati nelle T&C potrà farlo anche senza bisogno di preavviso (sospensione della collaborazione "per giusta causa").	-Apple si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) a sua completa discrezione e senza l'obbligo di procedere nell'avviso preventivo al cliente (esempi di possibili cause scatenanti alla base di tali provvedimenti sono indicate nei T&C). -Il cliente può decidere di terminare in qualsiasi momento l'uso del servizio senza alcun obbligo di preavviso.	-Dropbox si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) a sua completa discrezione e senza l'obbligo di procedere nell'avviso preventivo al cliente (anche se, solitamente, tale avviso viene fatto). -Il cliente può decidere di terminare in qualsiasi momento l'uso del servizio senza alcun obbligo di preavviso.
PRESERVAZIONE/ CANCELLAZIONE DATI AL TERMINE DELLA COLLABORAZIONE	Al termine della collaborazione Akamai procederà alla cancellazione dei dati del cliente a meno che non siano necessari per risolvere questioni legali.	I dati vengono conservati per 30 giorni dalla fine della collaborazione. Il cliente potrà recuperarli a patto di essere in regola con i pagamenti dovuti per il servizio (in caso, però, di fine del contratto per condotta del cliente non in linea con i termini previsti, il provider non procederà alla conservazione dei dati).	Al termine della collaborazione, l'utente non potrà più accedere ai servizi e ai dati presenti in essi, in quanto verranno istantaneamente rimossi. Per questo Apple consiglia un back-up continuo degli stessi.	Dropbox si riserva il diritto di poter rimuovere ogni tipo di contenuto all'interno dei propri servizi, a sua completa discrezione. Una volta terminata la collaborazione, solitamente, Dropbox si impegna per consentire al cliente il recupero dei dati prima della cancellazione, ma non si assume la responsabilità di farlo. La cancellazione dei dati avviene in tutti i casi in cui non vi siano ragioni legislative alla base della conservazione degli stessi o nel caso non siano condivisi con altri utenti.

FACEBOOK	GOOGLE	IBM	MICROSOFT	RACKSPACE	SALESFORCE.COM
Nel caso non si tratti di modifiche di natura legale o amministrativa, Facebook darà 7 giorni di preavviso al cliente pubblicando la futura variazione del T&C sulla "Pagina delle normative" del proprio sito (e consentendo commenti sulla stessa); il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.	Le variazioni agli originari termini contrattuali sono consentite e divengono effettive solamente se in forma scritta e firmate in calce sia dal provider, sia dal cliente (solo in caso di servizi cloud a pagamento).	Se vengono fatte, il provider aggiornerà i T&C sul sito web (in caso di norme riguardanti la "privacy" sarà indicato sul sito stesso un preavviso di 30 giorni al cambiamento che verrà) e da quel momento, tali modifiche, diverranno effettive; il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.	Se vengono fatte, il provider aggiornerà i T&C sul sito web e, in presenza di servizi a pagamento, si impegnerà nell'informare tempestivamente i clienti del cambiamento avvenuto (solitamente via e-mail); il cliente, a questo punto, ha 30 giorni a disposizione per recedere dal contratto. Se entro questo termine non dovesse compiere alcuna azione, si riterrà che abbia fornito un tacito assenso ai cambiamenti operati dal provider.	Se vengono fatte, il provider aggiornerà i T&C sul sito web e da quel momento, tali modifiche, diverranno effettive; il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.	Le variazioni agli originari termini contrattuali sono consentite e divengono effettive solamente se in forma scritta e firmate in calce sia dal provider, sia dal cliente (solo in caso di servizi cloud a pagamento).
-Facebook si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) nel caso di condotta illegale o non in linea con i T&C del contratto che regolano l'utilizzo del servizio. Se ciò avviene, Facebook invierà un'e-mail di notifica per annunciare il provvedimento preso. -Il cliente può decidere di terminare in qualsiasi momento l'uso del servizio senza alcun obbligo di preavviso.	-Google si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) a sua completa discrezione e senza l'obbligo di procedere nell'avviso preventivo al cliente (anche se, solitamente, tale avviso viene inoltrato). -Il cliente può decidere di terminare in qualsiasi momento l'uso del servizio senza alcun obbligo di preavviso.	-IBM si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) a sua completa discrezione e senza l'obbligo di procedere nell'avviso preventivo al cliente (anche se, solitamente, tale avviso viene fatto). -Il cliente può decidere di terminare in qualsiasi momento l'uso del servizio senza alcun obbligo di preavviso.	-Microsoft si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto e di procedere alla cancellazione dei dati del cliente, nel caso non vengano rispettati i T&C contrattuali (o per altri motivi per cui lo ritenga necessario) e senza l'obbligo di procedere nell'avviso preventivo al cliente (anche se, solitamente, tale avviso viene fatto). Per i "servizi a pagamento", se prima di 30 giorni dalla scadenza del contratto, il cliente non afferma di non volere continuare il rapporto, il rinnovo dello stesso avverrà automaticamente. -In generale, il cliente può decidere di terminare in qualsiasi momento l'uso del servizio.	-Rackspace si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) nel caso di condotta illegale o non in linea con i T&C del contratto che regolano l'utilizzo del servizio. -Il cliente può decidere di terminare in qualsiasi momento l'uso del servizio senza alcun obbligo di preavviso.	-Ognuna delle parti può recedere se l'altro contraente non rispetta uno o più accordi contrattuali e perseverà nel comportamento doloso per i 30 giorni susseguenti l'avviso ricevuto dalla controparte. In tal caso, se a recedere è il cliente egli avrà diritto al rimborso delle quote preversate per il godimento del servizio dal momento in cui recede a quando tale servizio avrebbe dovuto terminare secondo contratto; se a recedere è il provider, egli avrà diritto a trattenere (se già pagate) o a pretendere (se ancora da pagare) le somme dovute dal cliente dal momento in cui recede a quando tale servizio avrebbe dovuto terminare secondo contratto. -Se prima di 30 giorni dalla scadenza del contratto, uno dei contraenti non afferma di non volere continuare il rapporto, il rinnovo dello stesso avverrà automaticamente.
Qualora l'utente decidesse di eliminare il suo account, i contenuti al suo interno rimarranno ancora disponibili per un mese circa (a meno che tali contenuti non siano stati condivisi con terzi e che questi non li abbiano eliminati). Oltretutto è possibile che i contenuti rimossi vengano conservati come copie di back-up per circa 90 giorni (pur non essendo visibili ad altri).	Google si riserva di poter cancellare, a sua completa discrezione e in ogni momento, i dati immessi dal cliente all'interno delle sue piattaforme cloud. Al termine della collaborazione, inoltre, il provider manterrà il diritto di utilizzo, per fini commerciali, dei dati del cliente. Comunque, ove possibile, in caso di interruzione del rapporto stabilita dal provider, quest'ultimo provvederà a fornire un preavviso al cliente, il quale potrà accedere ai propri dati per il reintegro e poi ordinarne la cancellazione.	Al termine della collaborazione IBM procederà alla cancellazione dei dati del cliente a meno che non siano necessari per risolvere questioni legali.	-Microsoft si riserva il diritto di poter rimuovere ogni tipo di contenuto all'interno dei propri servizi, qualora lo ritenga in contrasto con la legge o con i T&C del contratto, ecceda i limiti di spazio consentiti o sia presente all'interno di un account non utilizzato per 270 giorni consecutivi. -Al termine della collaborazione Microsoft procederà alla cancellazione dei dati del cliente a meno che non siano necessari per risolvere questioni legali. Essa raccomanda, quindi, di conservare sempre una copia degli stessi. -Allo stesso tempo, Microsoft sottolinea che, anche se il contenuto non fosse più accessibile al cliente, potrebbe esserlo per il provider, essendoci la possibilità che rimanga, per un periodo indefinito, all'interno dei suoi sistemi, nonostante la fine della collaborazione.	Nessun riferimento specifico.	I dati vengono conservati per 30 giorni dalla fine della collaborazione e saranno disponibili su richiesta esplicita del cliente. Una volta trascorso tale periodo, se non espressamente impedito dalla legge, il provider procederà alla loro completa cancellazione.

Tabella 4.1: Confronto dei T&C contrattuali di 10 tra i più rinomati cloud provider a livello internazionale.

4.2 Gli elementi che impattano sulla sicurezza nei contratti cloud

Dopo aver esaminato, nel dettaglio, i vari aspetti che caratterizzano un tipico contratto di cloud computing, é il momento di focalizzarci sugli elementi, all'interno dello stesso, che impattano direttamente sulla sicurezza del cliente.

Gli elementi che impattano sulla sicurezza all'interno dei contratti cloud sono riconducibili a tre categorie principali, tutte riguardanti, esplicitamente, i dati immessi dal cliente all'interno delle piattaforme del provider; *confidentiality*, *integrity* e *availability.*

Vediamone, qui di seguito, il preciso significato e i relativi vari aspetti da considerare:

- *Confidentiality:* la "confidentiality" fa riferimento all'insieme di regole e misure mirate a limitare l'accesso ai dati di esclusiva proprietà del cliente.

  Essa dipende, tipicamente, dal livello di privacy di cui il cliente ha bisogno e, a livello concreto, si occupa di fare in modo che i dati sensibili non cadano in mano alle persone sbagliate, che potrebbero farne un uso improprio/illegale o, comunque, non autorizzato.

  La "data encryption"[20] é, ad esempio, una tipica misura adottata per preservare il carattere confidenziale dei dati all'interno delle piattaforme cloud.

20 Vedi Capitolo 4, pag. 140.

- *Integrity:* l' ”integrity” si riferisce alla necessità di assicurare la consistenza, precisione e affidabilità dei dati per l'intero periodo di collaborazione tra cloud provider e cliente.

  Serve, quindi, che il provider si accerti che nessun elemento venga alterato da persone a cui non é consentito compiere un'azione simile.

  Inoltre é buona abitudine procedere ad un back-up periodico dei dati stessi che ne possa scongiurare la perdita (parziale o totale), in seguito ad inconvenienti imprevedibili (non imputabili all'azione dell'uomo), che portino alla rottura o al malfunzionamento del server (momentaneamente o permanentemente).

- *Availability:* l' ”availability” (letteralmente “disponibilità” dei dati) riguarda l'accesso alle informazioni che si necessitano da parte dei soggetti autorizzati e il tempo che trascorre dal momento della richiesta, all'effettiva consultazione. Per fare in modo che essa venga costantemente garantita, occorrono una rigorosa manutenzione delle varie componenti hardware in gioco, un pronto riparo delle stesse se ce ne fosse il bisogno, la disponibilità di una banda larga adeguata al traffico previsto, il possesso di un efficace sistema dedito al back-up, un costante impegno nel procedere all'aggiornamento continuo dei propri software e un adeguato insieme di meccanismi in funzione finalizzati alla protezione da attacchi esterni (come, ad esempio, i DDoS[21]). (-Sandeep K. Sood, *“A combined approach to ensure data security in cloud computing”*,

21 Vedi Capitolo 4, pag. 137.

Journal of Network and Computer Applications, 2012-) (-Margaret Rouse, *"Confidentiality, Integrity and Availability"*, whatis.techtarget.com, 2013-)

Ora, concentrandoci su questi tre aspetti fondamentali per definire la sicurezza all'interno di un contratto di cloud computing, analizzeremo, uno per uno, i 10 provider presi in considerazione nella tabella 4.1 (Akamai, Amazon, Apple, Dropbox, Facebook, Google, IBM, Microsoft, Rackspace e Salesforce.com) e, focalizzandoci su alcune precise categorie (la responsabilità del provider nella fornitura dei servizi e per l'integrità dei dati, il diritto all'utilizzo dei dati del cliente, l'eventuale indennizzo a favore del consumatore, le garanzie e la preservazione/cancellazione dei dati), delineeremo un profilo in termini di sicurezza per ciascuno di essi (assegnando una valutazione alle componenti di confidentiality, integrity e availability che, in scala crescente, potrà andare dall' "inadeguata", alla "sufficiente", alla "buona", alla "ottima"), seguito, poi, da una rappresentazione grafica che ne permetterà il vicendevole confronto.

4.2.1 Akamai

Akamai Technologies é un'azienda che fornisce una piattaforma per la distribuzione di contenuti via internet.

Situata a Cambridge, nello stato del Massachusetts (USA), é stata fondata nel 1998 da Daniel Lewin (appena laureatosi al “Massachusetts Institute of Technology”), da un professore, Tom Leighton, e da altri due studenti.

- ***Confidentiality:*** *buona.*

  Akamai specifica, all'interno dei propri “Terms & Conditions” contrattuali, che non condividerà alcun dato di proprietà dei clienti con terzi, se non dopo loro esplicita autorizzazione (eccetto nel caso in cui i dati fossero richiesti dalla legge o in situazioni particolari di pubblico interesse; in tali situazioni il provider diffonderà i dati del cliente anche senza preavviso e assenso di quest'ultimo).

  Allo stesso tempo, però, non fornisce nessun tipo di garanzia sull'effettiva riuscita dei meccanismi posti in atto per la conservazione del carattere confidenziale dei dati stessi e, se ritenuta colpevole dalla legge per l'accesso a tali informazioni da parte di soggetti non autorizzati, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare ciò che il cliente ha versato nei 6 mesi precedenti la domanda di indennizzo.

- ***Integrity:*** *sufficiente.*

  Akamai specifica, all'interno dei propri "Terms & Conditions" contrattuali, che adotterà misure all'avanguardia per preservare l'integrità dei dati.

  Tuttavia non fornisce alcuna garanzia sulla riuscita di tali misure e, ove permesso dalla legge, declina ogni responsabilità derivante da perdite/danni ragionevolmente prevedibili, causati al cliente dall'alterazione/manomissione dei suoi dati da parte di terzi non autorizzati.

  Nel caso in cui Akamai venisse dichiarata colpevole dalla legge, la sua responsabilità si limiterà ad un rimborso di una quota che non potrà, comunque, mai superare ciò che il cliente ha versato nei 6 mesi precedenti la domanda di indennizzo.

- ***Availability:*** *buona.*

  Akamai specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si impegnerà ad offrire i servizi richiesti come in essi descritto e, per ciò che riguarda le variazioni ai termini contrattuali (che possono incidere direttamente sull'availability), indica che sono consentite e divengono effettive solamente se in forma scritta e firmate in calce sia dal provider, sia dal cliente.

  Se, però, il cliente non rispettasse uno o più accordi contrattuali e perseverasse nel comportamento doloso per 30 giorni consecutivi, Akamai potrà terminare il servizio istantaneamente. A ciò va aggiunto che, se prima di 60 giorni dalla scadenza della collaborazione, il cliente non affermasse di non volere

continuare il rapporto, il rinnovo dello stesso avverrà automaticamente.

Infine, Akamai precisa che, al termine della collaborazione, procederà all'immediata cancellazione dei dati del cliente, a meno che la loro ulteriore conservazione non sia richiesta per motivi legali. La mancanza, quindi, di un periodo a disposizione del cliente per il recupero del proprio "contenuto informativo" consiglia, dunque, operazioni di back-up costanti, che scongiurino la perdita dello stesso in caso di interruzioni del rapporto provider-cliente non preventivate/preventivabili.

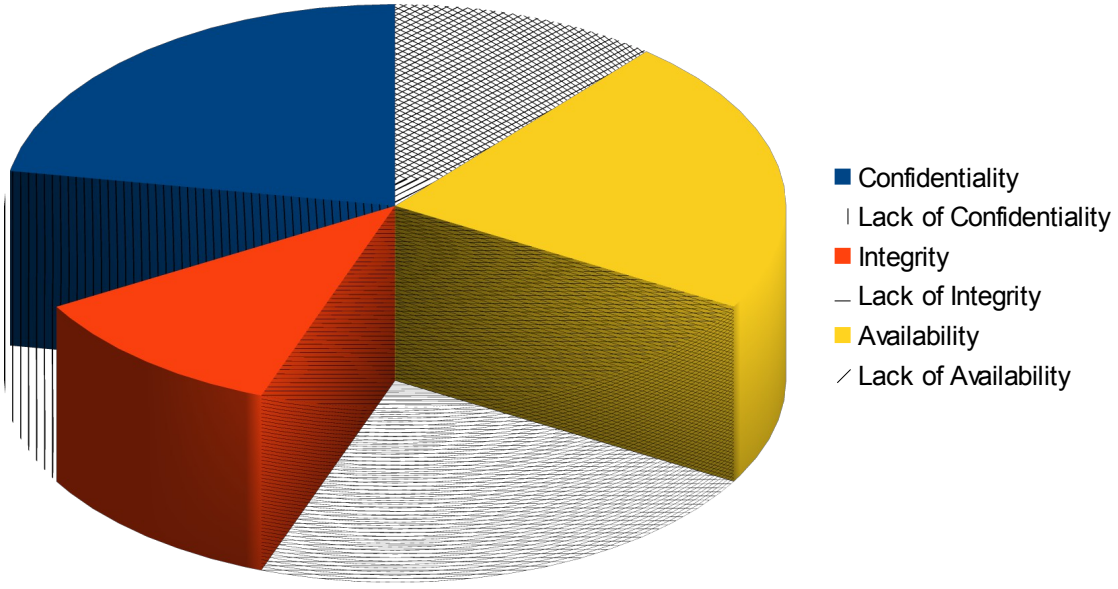

Grafico 4.1: La confidentiality, l'integrity e l'availability nei T&C di Akamai.

4.2.2 Amazon

Amazon é un'azienda di commercio elettronico statunitense con sede a Seattle, nello stato di Washington.

Fondata con il nome di “Cadabra.com” da Jeff Bezos nel 1994 e lanciata nel 1995, Amazon iniziò come libreria online, ma presto allargò la gamma dei propri prodotti venduti a DVD, CD musicali, software, videogiochi, prodotti elettronici, abbigliamento, mobilia, cibo, giocattoli, ecc...

L'azienda ha provveduto a creare, nel tempo, siti similari in svariate altre nazioni e spedisce i suoi prodotti in tutto il mondo.

- ***Confidentiality:*** *sufficiente.*

  Amazon non indica, all'interno dei propri “Terms & Conditions” contrattuali, che non diffonderà i dati del cliente a terzi, bensì che ne farà un utilizzo consono allo scopo per cui essi sono stati resi disponibili sulle sue piattaforme. In tutti gli altri casi, invece, chiederà, preventivamente, un'autorizzazione al cliente (nel caso in cui fossero richiesti dalla legge, però, il provider diffonderà i dati del cliente anche senza preavviso e assenso di quest'ultimo). Così facendo, non stabilendo dei confini precisi di condotta nell'utilizzo degli elementi forniti dal consumatore, Amazon si riserva un determinato ammontare di arbitrarietà nella gestione degli stessi.

  Allo stesso tempo non fornisce nessun tipo di garanzia sull'effettiva riuscita dei

meccanismi posti in atto per la conservazione del carattere confidenziale dei dati stessi e, se ritenuta colpevole dalla legge per l'accesso a tali informazioni da parte di soggetti non autorizzati, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare ciò che il cliente ha versato nei 12 mesi precedenti la domanda di indennizzo.

- ***Integrity:*** *sufficiente.*

  Amazon specifica, all'interno dei propri "Terms & Conditions" contrattuali, che adotterà misure all'avanguardia per preservare l'integrità dei dati.

  Tuttavia non fornisce alcuna garanzia sulla riuscita di tali misure e, ove permesso dalla legge, declina ogni responsabilità derivante da perdite/danni ragionevolmente prevedibili, causati al cliente dall'alterazione/manomissione dei suoi dati da parte di terzi non autorizzati.

  Nel caso in cui Amazon venisse dichiarata colpevole dalla legge, la sua responsabilità si limiterà ad un rimborso di una quota che non potrà, comunque, mai superare ciò che il cliente ha versato nei 12 mesi precedenti la domanda di indennizzo.

- ***Availability:*** *sufficiente.*

  Amazon specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si impegnerà a fornire i servizi richiesti come indicato in essi, ma che il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricadrà interamente sul cliente. Per ciò che riguarda le variazioni ai termini contrattuali

(che possono incidere direttamente sull'availability), indica che, nel caso in cui vengano fatte, provvederà ad aggiornare i T&C sul proprio sito web (informando, preventivamente, il cliente via e-mail se si trattasse di servizi cloud a pagamento) e, da quel momento, tali modifiche diverranno effettive; il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.

Amazon, inoltre, si riserva, a sua completa discrezione, il diritto di terminare il servizio qualora lo ritenga necessario (sospensione della collaborazione "per convenienza"); in questo caso, però, dovrà fornire al cliente 30 giorni di preavviso in merito alla decisione presa. Se, invece, il cliente non rispettasse uno o più accordi contrattuali e perseverasse nel comportamento doloso per 30 giorni consecutivi, Amazon potrà terminare il servizio immediatamente, senza alcun bisogno di preavviso.

Infine, al termine della collaborazione, Amazon concederà 30 giorni al cliente per recuperare i propri dati (a patto che sia in regola con i pagamenti dovuti), prima di procedere alla loro cancellazione. Se, però, ci si trovasse in una situazione di "fine del contratto dovuta a comportamenti del cliente non in linea con i termini previsti", il provider non sarà tenuto alla postuma temporanea conservazione dei dati e potrà procedere all'immediata rimozione degli stessi.

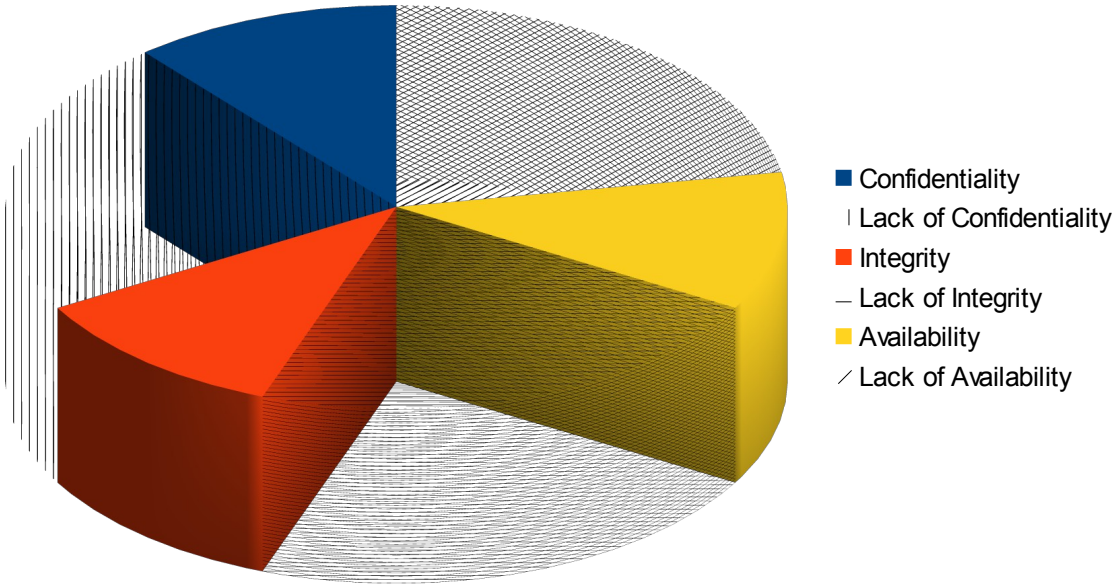

Grafico 4.2: La confidentiality, l'integrity e l'availability nei T&C di Amazon.

4.2.3 Apple

Apple é un'azienda informatica statunitense che produce sistemi operativi, computer, e dispositivi multimediali, con sede a Cupertino, nello stato della California.
Fondata nel 1976 da Steve Jobs, Steve Wozniak e Ronald Wayne e conosciuta a livello mondiale sin dai primi anni ottanta grazie alla vasta gamma di computer Macintosh, attualmente il suo nome é associato anche al lettore di musica digitale iPod, al negozio di musica online iTunes Store, all'iPhone (tipo di smartphone basato sul sistema operativo iOS) e al tablet iPad.

- ***Confidentiality:*** *sufficiente.*

  Apple non indica, all'interno dei propri "Terms & Conditions" contrattuali, che non diffonderà i dati del cliente a terzi, bensì che ne farà un utilizzo consono allo scopo per cui essi sono stati resi disponibili sulle sue piattaforme.

  In tutti gli altri casi, invece, chiederà, preventivamente, un'autorizzazione al cliente (nel caso in cui fossero richiesti dalla legge o siano fondamentali per tutelare la sicurezza e l'immagine sua e/o quella della propria clientela, però, il provider diffonderà i dati del cliente anche senza preavviso e assenso di quest'ultimo). Così facendo, non stabilendo dei confini precisi di condotta nell'utilizzo degli elementi forniti dal consumatore, Apple si riserva un determinato ammontare di arbitrarietà nella gestione degli stessi.

  Allo stesso tempo essa specifica, in modo chiaro, che non fornisce nessun tipo

di garanzia sull'effettiva riuscita dei meccanismi posti in atto per la conservazione del carattere confidenziale dei dati stessi.

- ***Integrity:*** *inadeguata.*

  Apple specifica, all'interno dei propri "Terms & Conditions" contrattuali, che adotterà misure all'avanguardia per preservare l'integrità dei dati.

  Tuttavia non fornisce alcuna garanzia sulla riuscita di tali misure e, ove permesso dalla legge, declina ogni responsabilità derivante dall'alterazione/manomissione dei dati del cliente da parte di terzi non autorizzati.

- ***Availability:*** *inadeguata.*

  Apple specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si impegnerà a fornire i servizi richiesti come indicato in essi, ma che il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricadrà interamente sul cliente. Per ciò che riguarda le variazioni ai termini contrattuali (che possono incidere direttamente sull'availability), indica che, nel caso in cui vengano fatte, provvederà ad aggiornare i T&C sul proprio sito web e, da quel momento, tali modifiche diverranno effettive; il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.

  Apple, inoltre, si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) a sua

completa discrezione e senza l'obbligo di procedere nell'avviso preventivo al cliente (esempi di possibili cause scatenanti alla base di tali provvedimenti sono indicate nei T&C).

Infine, al termine della collaborazione, Apple procederà all'istantanea rimozione dell'intero ammontare dei dati del cliente presenti all'interno delle proprie piattaforme, non consentendo, quindi, ulteriori accessi finalizzati al reintegro degli stessi; per questo motivo essa é solita consigliare caldamente, all'intero bacino di utenza, un back-up continuo dell'intero contenuto presente all'interno dei suoi servizi.

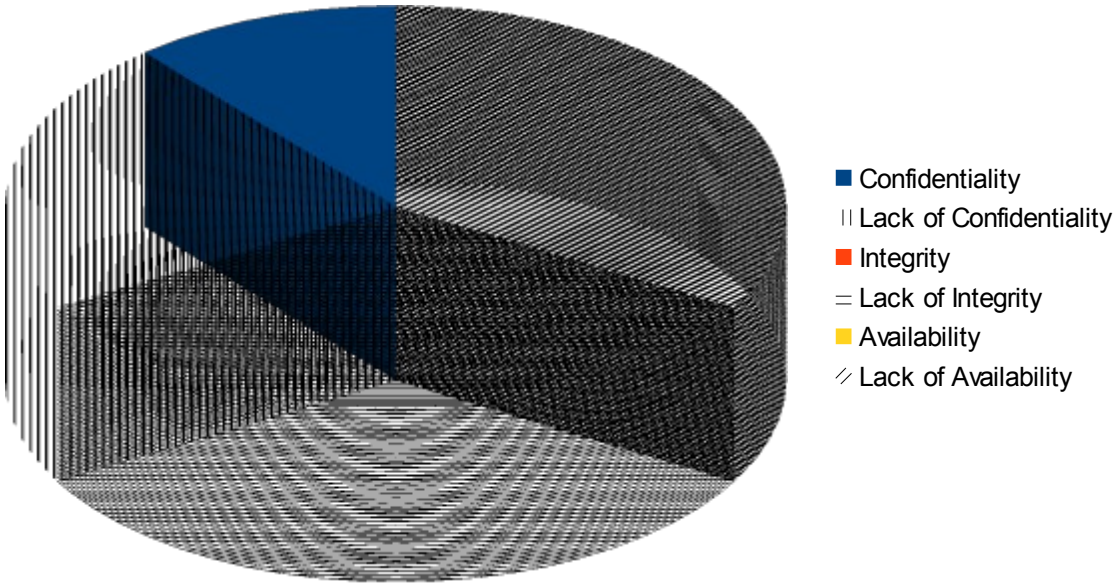

Grafico 4.3: La confidentiality, l'integrity e l'availability nei T&C di Apple.

4.2.4 Dropbox

Dropbox é un'azienda specializzata in software di cloud storage multipiattaforma che offre un servizio di file hosting e sincronizzazione automatica di file tramite web, con sede a San Francisco, nello stato della California (USA).

La sua fondazione, da parte di Drew Houston e Arash Ferdowsi, risale al 2007, sotto forma di start-up finanziata dal ventur capitalist “Y Combinator”.

- ***Confidentiality:*** *buona.*

  Dropbox specifica, all'interno dei propri “Terms & Conditions” contrattuali, che non condividerà alcun dato di proprietà dei clienti con terzi, se non dopo loro esplicita autorizzazione (eccetto nel caso in cui fossero richiesti dalla legge o siano fondamentali per tutelare la sicurezza e l'immagine sua e/o quella della propria clientela; in tali situazioni il provider diffonderà i dati del cliente anche senza preavviso e assenso di quest'ultimo).

  Allo stesso tempo, però, non fornisce nessun tipo di garanzia sull'effettiva riuscita dei meccanismi posti in atto per la conservazione del carattere confidenziale dei dati stessi e, se ritenuta colpevole dalla legge per l'accesso a tali informazioni da parte di soggetti non autorizzati, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare i $20 oppure ciò che il cliente ha versato nei 3 mesi precedenti la domanda di indennizzo.

- ***Integrity:*** *sufficiente.*

  Dropbox specifica, all'interno dei propri "Terms & Conditions" contrattuali, che adotterà misure all'avanguardia per preservare l'integrità dei dati.

  Tuttavia non fornisce alcuna garanzia sulla riuscita di tali misure e, ove permesso dalla legge, declina ogni responsabilità derivante da perdite/danni ragionevolmente prevedibili, causati al cliente dall'alterazione/manomissione dei suoi dati da parte di terzi non autorizzati.

  Nel caso in cui Dropbox venisse dichiarata colpevole dalla legge, la sua responsabilità si limiterà ad un rimborso di una quota che non potrà, comunque, mai superare i $20 oppure ciò che il cliente ha versato nei 3 mesi precedenti la domanda di indennizzo.

- ***Availability:*** *inadeguata.*

  Dropbox specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si impegnerà a fornire i servizi richiesti come indicato in essi, ma che il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricadrà interamente sul cliente. Per ciò che riguarda le variazioni ai termini contrattuali (che possono incidere direttamente sull'availability), indica che, nel caso in cui vengano fatte, provvederà ad aggiornare i T&C sul proprio sito web (se si trattasse di "modifiche importanti" e di servizi a pagamento informerà precedentemente il cliente via e-mail) e, da quel momento, tali modifiche diverranno effettive; il continuo utilizzo del servizio da parte del cliente

rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.

Dropbox, inoltre, si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) a sua completa discrezione e senza l'obbligo di procedere nell'avviso preventivo al cliente (anche se, solitamente, tale avviso viene inoltrato).

Infine, Dropbox specifica che sarà autorizzata a rimuovere ogni tipo di contenuto all'interno dei propri servizi, a sua completa discrezione. Una volta terminata la collaborazione, nella gran parte dei casi, Dropbox si impegna per consentire al cliente il recupero dei dati prima della cancellazione, ma non si assume la responsabilità di farlo. A prescindere da ciò, la cancellazione degli stessi, o prima o dopo, avviene in tutti i casi in cui non vi siano ragioni legislative alla base della loro conservazione o condivisioni con altri utenti.

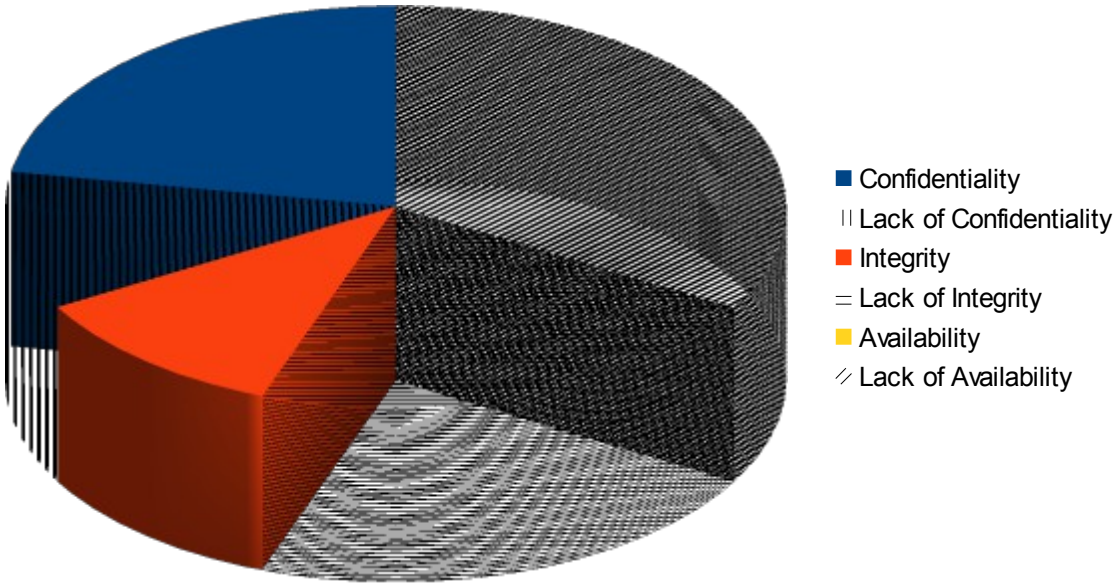

Grafico 4.4: La confidentiality, l'integrity e l'availability nei T&C di Dropbox.

4.2.5 Facebook

Facebook é un servizio di rete sociale fondato ad Harvard, negli Stati Uniti, nel febbraio 2004, da Mark Zuckerberg e dai suoi compagni di università Eduardo Saverin, Dustin Moskovitz e Chris Hughes. Originariamente era stato progettato esclusivamente per gli studenti dell'università di Harvard, ma la sua diffusione fu ben presto più ampia.

Al giorno d'oggi é disponibile in oltre 70 lingue e conta più di un miliardo di utenti che effettuano l'accesso almeno una volta al mese, classificandosi come primo servizio di rete sociale per numero di utenti attivi.

- ***Confidentiality:*** *inadeguata.*

  Facebook specifica, all'interno dei propri "Terms & Conditions" contrattuali, che l'utente, una volta pubblicato del contenuto all'interno del proprio profilo, concede una licenza non esclusiva, trasferibile, nell'utilizzo, a discrezione del provider, dello stesso. Tale utilizzo terminerà solo qualora l'utente elimini il suo account (o i contenuti al suo interno), a meno che tali contenuti non siano stati condivisi con terzi e che questi non li abbiano eliminati a loro volta. Oltretutto viene precisato che é possibile che i dati rimossi vengano conservati come copie di back-up per circa 90 giorni (pur non essendo visibili ad altri se non al provider).

  Allo stesso tempo Facebook non fornisce nessun tipo di garanzia e, se ritenuta colpevole dalla legge per l'accesso ad informazioni sensibili della propria

clientela da parte di soggetti non autorizzati, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare i $100.

- ***Integrity:*** *inadeguata.*

  Facebook specifica, all'interno dei propri "Terms & Conditions" contrattuali, che non fornirà alcuna garanzia sull'integrità dei dati della clientela durante l'utilizzo dei propri servizi.

- ***Availability:*** *sufficiente.*

  Facebook specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si impegnerà a fornire i servizi richiesti come indicato in essi, ma che il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricadrà interamente sul cliente. Per ciò che riguarda le variazioni ai termini contrattuali (che possono incidere direttamente sull'availability), indica che, nel caso non si tratti di modifiche di natura legale o amministrativa, si premurerà di dare 7 giorni di preavviso alla clientela, pubblicando la futura variazione dei T&C sulla "Pagina delle normative" del proprio sito web (e consentendo i commenti dell'utenza alla stessa); il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.

  Facebook, inoltre, si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso), nel caso di condotta illegale o non in linea con i T&C del contratto che regolano l'utilizzo

del servizio. Se ciò dovesse verificarsi, il provider invierà un'e-mail di notifica all'utente per annunciare il provvedimento preso.

Infine, Facebook precisa che, qualora l'utente decidesse di eliminare il proprio account, i contenuti al suo interno rimarranno ancora disponibili per un mese circa (a meno che tali contenuti non siano stati condivisi con terzi e che questi non li abbiano eliminati a loro volta). Specifica, in aggiunta, che é possibile che i contenuti rimossi vengano conservati come copie di back-up per circa 90 giorni (pur non essendo visibili ad altri se non al provider).

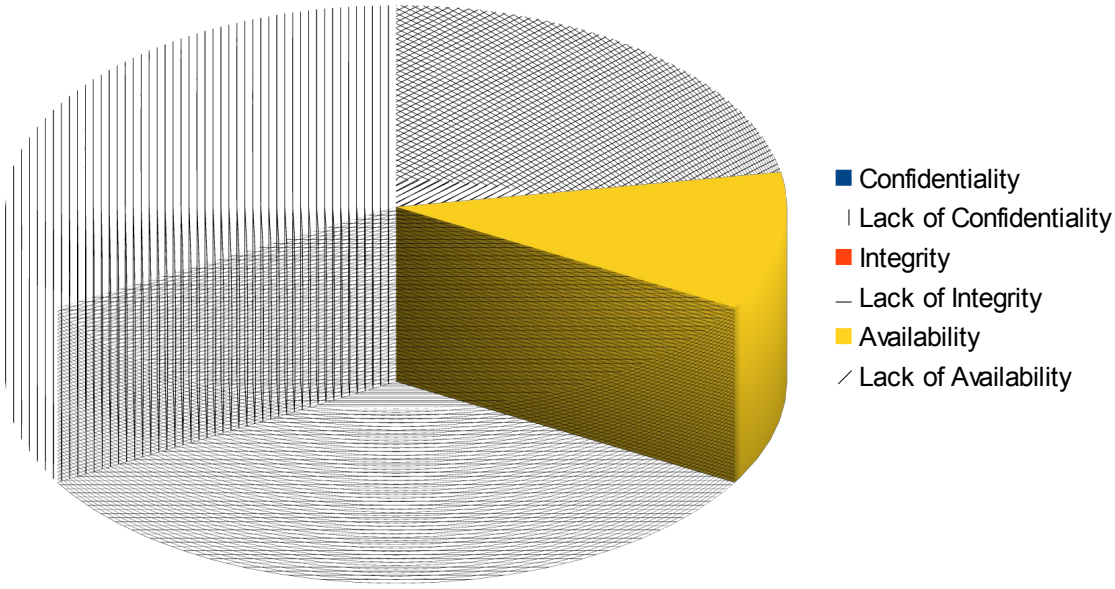

Grafico 4.5: La confidentiality, l'integrity e l'availability nei T&C di Facebook.

4.2.6 Google

Google é una multinazionale americana specializzata in servizi e prodotti legati ad internet come la ricerca sul web, il cloud computing, i software e tecnologie varie collegate alla pubblicità online.

Fondata il 27 settembre 1998 da Larry Page e Sergej Brin, all'epoca studenti dell'università di Stanford, ha, attualmente, il proprio quartier generale a Mountain View, nello stato della California.

- ***Confidentiality:*** *inadeguata.*

  Google specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si riserva il diritto di usufruire dei dati del cliente a suo piacimento per ciò che concerne l'utilizzo, la promozione, il miglioramento e lo sviluppo dei propri servizi, secondo i principi indicati nelle "norme sulla privacy" (eccetto nel caso in cui fossero richiesti dalla legge o siano fondamentali per tutelare la sicurezza e l'immagine sua e/o quella della propria clientela; in tali situazioni il provider li diffonderà comunque).

  Allo stesso tempo, però, non fornisce nessun tipo di garanzia sull'effettiva riuscita dei meccanismi posti in atto per la conservazione del carattere confidenziale dei dati stessi e, se ritenuta colpevole dalla legge per l'accesso a tali informazioni da parte di soggetti non autorizzati, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare

l'intero ammontare versato per l'utilizzo dei servizi, precedente la domanda di indennizzo.

Infine, Google precisa che, al termine della collaborazione, manterrà il diritto di utilizzo, per fini commerciali, del contenuto immesso dal cliente.

- ***Integrity:*** *sufficiente.*

  Google specifica, all'interno dei propri "Terms & Conditions" contrattuali, che adotterà misure all'avanguardia per preservare l'integrità dei dati.

  Tuttavia non fornisce alcuna garanzia sulla riuscita di tali misure e, ove permesso dalla legge, declina ogni responsabilità derivante da perdite/danni ragionevolmente prevedibili, causati al cliente dall'alterazione/manomissione dei suoi dati da parte di terzi non autorizzati.

  Nel caso in cui Google venisse dichiarata colpevole dalla legge, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare l'ammontare versato per l'utilizzo dei servizi, precedente la domanda di indennizzo.

- ***Availability:*** *sufficiente.*

  Google specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si impegnerà a fornire i servizi richiesti come indicato in essi, ma che il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricadrà interamente sul cliente.

  Per ciò che riguarda le variazioni ai termini contrattuali (che possono incidere

direttamente sull'availability), indica che sono consentite e divengono effettive solamente se in forma scritta e firmate in calce sia dal provider, sia dal cliente. Google, inoltre, si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) a sua completa discrezione e senza l'obbligo di procedere nell'avviso preventivo al cliente (anche se, solitamente, tale avviso viene inoltrato).

Infine Google si riserva di poter cancellare, a sua completa discrezione e in ogni momento, i dati immessi dal cliente all'interno delle sue piattaforme cloud. Al termine della collaborazione, inoltre, il provider manterrà il diritto di utilizzo, per fini commerciali, del contenuto immesso dal cliente.

Va precisato, però, che, ove possibile, in caso di interruzione del rapporto stabilita dal provider, quest'ultimo provvederà a fornire un preavviso al cliente, il quale potrà accedere ai propri dati per il reintegro; solo allora Google provvederà ad ordinarne la cancellazione.

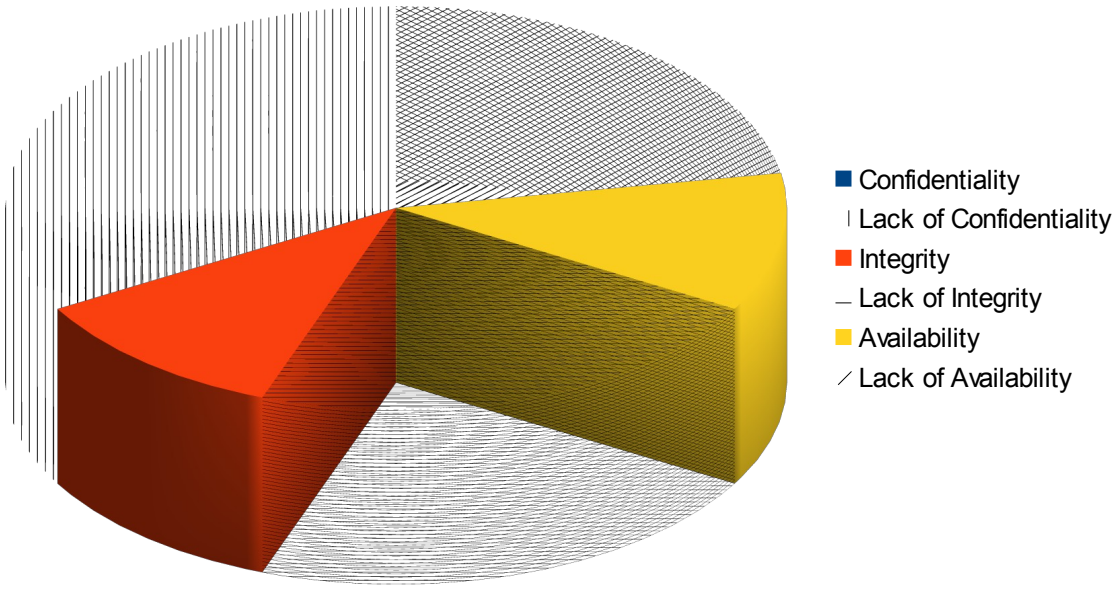

Grafico 4.6: La confidentiality, l'integrity e l'availability nei T&C di Google.

4.2.7 IBM

IBM (International Business Machines Corporation) é un'azienda statunitense tra le maggiori al mondo nel settore informatico; produce e commercializza hardware e software, offre infrastrutture, servizi di hosting e consulenza in settori che spaziano dai mainframe alle nanotecnologie.

Fondata nel 1911 come derivante dalla fusione di tre diverse aziende, adottò il nome attuale solo nel 1924; attualmente ha sede ad Armonk, nello stato di New York e, a partire da settembre 2011, é la seconda più grande azienda tecnologica al mondo quotata in borsa per capitalizzazione di mercato.

- ***Confidentiality:*** *sufficiente.*

  IBM non indica, all'interno dei propri "Terms & Conditions" contrattuali, che non diffonderà i dati del cliente a terzi, bensì che ne farà un utilizzo consono allo scopo per cui essi sono stati resi disponibili sulle sue piattaforme.

  In tutti gli altri casi, invece, chiederà, preventivamente, un'autorizzazione al cliente (nel caso in cui fossero richiesti dalla legge o siano fondamentali per tutelare la sicurezza e l'immagine sua e/o quella della propria clientela, però, il provider diffonderà i dati del cliente anche senza preavviso e assenso di quest'ultimo). Così facendo, non stabilendo dei confini precisi di condotta nell'utilizzo degli elementi forniti dal consumatore, IBM si riserva un determinato ammontare di arbitrarietà nella gestione degli stessi.

Allo stesso tempo essa specifica, in modo chiaro, che non fornisce nessun tipo di garanzia sull'effettiva riuscita dei meccanismi posti in atto per la conservazione del carattere confidenziale dei dati stessi.

- ***Integrity:*** *inadeguata.*

  IBM specifica, all'interno dei propri "Terms & Conditions" contrattuali, che adotterà misure all'avanguardia per preservare l'integrità dei dati.

  Tuttavia non fornisce alcuna garanzia sulla riuscita di tali misure e, ove permesso dalla legge, declina ogni responsabilità derivante dall'alterazione/manomissione dei dati del cliente, da parte di terzi non autorizzati.

- ***Availability:*** *inadeguata.*

  IBM specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si impegnerà a fornire i servizi richiesti come indicato in essi, ma che il rischio legato all'effettiva fornitura degli stessi e al loro contenuto ricadrà interamente sul cliente. Per ciò che riguarda le variazioni ai termini contrattuali (che possono incidere direttamente sull'availability), indica che, nel caso in cui vengano fatte, provvederà ad aggiornare i T&C sul proprio sito web (in caso di norme riguardanti la "privacy" sarà indicato sul sito stesso un preavviso di 30 giorni al cambiamento che verrà) e, da quel momento, tali modifiche diverranno effettive; il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal

cambiamento.

IBM, inoltre, si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) a sua completa discrezione e senza l'obbligo di procedere nell'avviso preventivo al cliente (anche se, solitamente, tale avviso viene inoltrato).

Infine, IBM specifica che, al termine della collaborazione, procederà all'immediata cancellazione dei dati del cliente, a meno che la loro ulteriore conservazione non sia richiesta per motivi legali. La mancanza, quindi, di un periodo a disposizione del cliente per il recupero del proprio "contenuto informativo", consiglia, dunque, operazioni di back-up costanti che scongiurino la perdita dello stesso in caso di interruzioni del rapporto provider-cliente non preventivate/preventivabili.

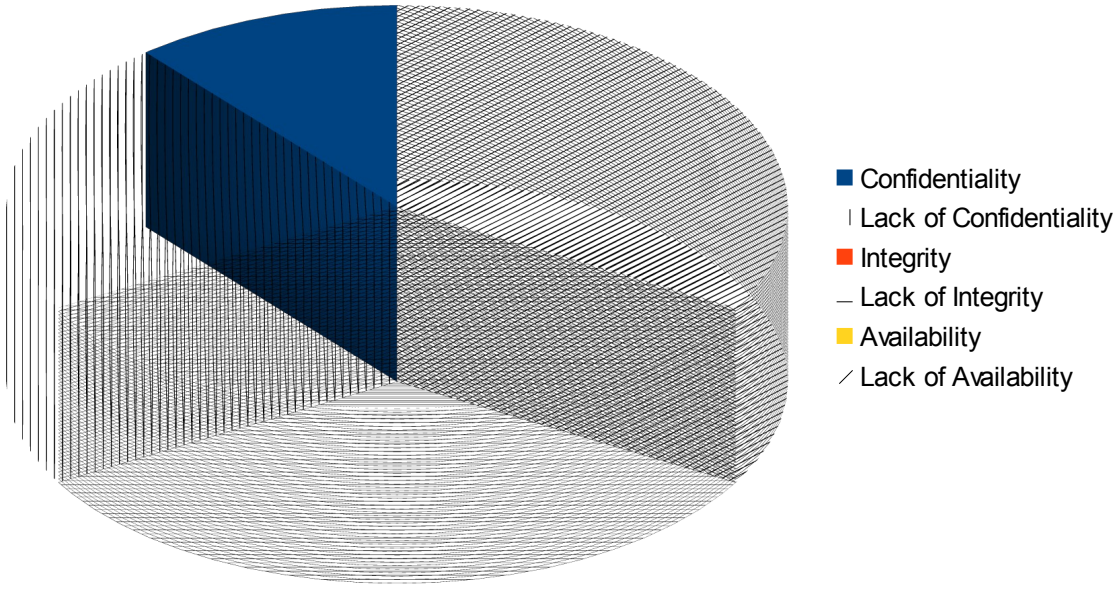

Grafico 4.7: La confidentiality, l'integrity e l'availability nei T&C di IBM.

4.2.8 Microsoft

Microsoft Corporation é una delle più importanti aziende d'informatica del mondo ed anche una delle più grandi imprese con una capitalizzazione azionaria superiore ai 260 miliardi di dollari.

Sviluppa, produce e vende prodotti che spaziano da personal computer, software ed altri componenti elettronico/informatici.

Fondata il 4 aprile 1975 da Bill Gates e Paul Allen, ha, attualmente, la propria sede a Redmond, nello stato di Washington (USA).

- ***Confidentiality:*** *sufficiente.*

  Microsoft specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si riserva il diritto di usufruire dei dati del cliente a suo piacimento per ciò che concerne l'utilizzo, la promozione, il miglioramento e lo sviluppo dei propri servizi (eccetto nel caso in cui fossero richiesti dalla legge o siano fondamentali per tutelare la sicurezza e l'immagine sua e/o quella della propria clientela; in tali situazioni il provider li diffonderà comunque).

  Allo stesso tempo, però, non fornisce nessun tipo di garanzia sull'effettiva riuscita dei meccanismi posti in atto per la conservazione del carattere confidenziale dei dati stessi e, se ritenuta colpevole dalla legge per l'accesso a tali informazioni da parte di soggetti non autorizzati, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare

l'intero ammontare versato per l'utilizzo dei servizi, precedente la domanda di indennizzo.

- ***Integrity:*** *sufficiente.*

  Microsoft specifica, all'interno dei propri "Terms & Conditions" contrattuali, che adotterà misure all'avanguardia per preservare l'integrità dei dati.

  Tuttavia non fornisce alcuna garanzia sulla riuscita di tali misure e, ove permesso dalla legge, declina ogni responsabilità derivante da perdite/danni ragionevolmente prevedibili, causati al cliente dall'alterazione/manomissione dei suoi dati da parte di terzi non autorizzati.

  Nel caso in cui Microsoft venisse dichiarata colpevole dalla legge, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare l'ammontare versato per l'utilizzo dei servizi, precedente la domanda di indennizzo.

- ***Availability:*** *buona.*

  Microsoft specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si ritiene responsabile per il mancato rispetto degli stessi, solo nel caso esso sia imputabile a suoi atti di negligenza. Precisa, inoltre, che se dovesse interrompere la fornitura del servizio al cliente senza "giusta causa", sarà suo dovere provvedere ad un rimborso della parte di servizio pagata, ma, poi, non fornita.

  Per ciò che riguarda le variazioni ai termini contrattuali (che possono incidere

direttamente sull'availability), indica che, nel caso in cui vengano fatte, provvederà ad aggiornare i T&C sul proprio sito web e, in presenza di servizi a pagamento, si impegnerà nell'informare tempestivamente i clienti del cambiamento avvenuto (solitamente via e-mail); il cliente, a questo punto, ha 30 giorni a disposizione per recedere dal contratto. Se entro questo termine non dovesse compiere alcuna azione, si riterrà che abbia fornito un tacito assenso ai cambiamenti operati dal provider.

Microsoft, inoltre, si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto, nel caso non vengano rispettati i T&C contrattuali (o per altri motivi per cui lo ritenga necessario) e senza l'obbligo di procedere nell'avviso preventivo al cliente (anche se, solitamente, tale avviso viene inoltrato). Per i servizi a pagamento, se prima di 30 giorni dalla scadenza del contratto, il cliente non afferma di non voler continuare il rapporto, il rinnovo dello stesso avverrà automaticamente.

In più, Microsoft “si autorizza” a rimuovere ogni tipo di contenuto all'interno dei propri servizi, qualora lo ritenga in contrasto con la legge o con i T&C del contratto, ecceda i limiti di spazio consentiti o sia presente all'interno di un account non utilizzato per 270 giorni consecutivi.

Infine Microsoft specifica che, al termine della collaborazione, procederà all'immediata cancellazione dei dati del cliente, a meno che la loro ulteriore conservazione non sia richiesta per motivi legali. La mancanza, quindi, di un periodo a disposizione del cliente per il recupero del proprio “contenuto

informativo", consiglia, dunque, operazioni di back-up costanti, che scongiurino la perdita dello stesso in caso di interruzioni del rapporto provider-cliente non preventivate/preventivabili. Allo stesso tempo Microsoft sottolinea che, anche se il contenuto non fosse più accessibile al cliente, potrebbe esserlo per il provider, essendoci la possibilità che rimanga all'interno dei suoi sistemi, per un periodo indefinito, nonostante la fine della collaborazione.

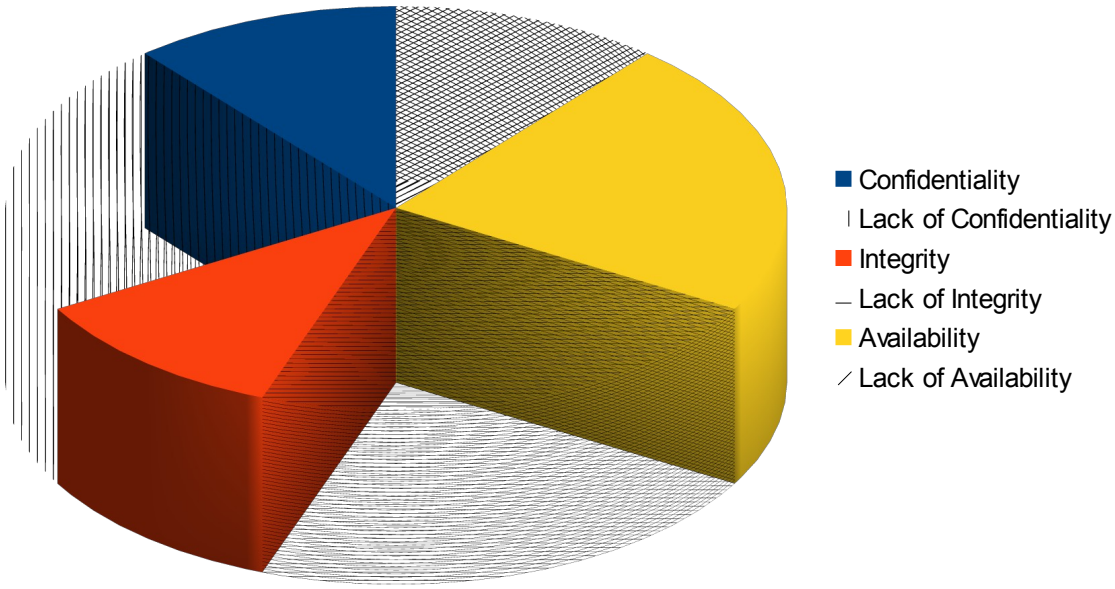

Grafico 4.8: La confidentiality, l'integrity e l'availability nei T&C di Microsoft.

4.2.9 Rackspace

Rackspace é un'azienda specializzata in “hybrid cloud” che fornisce una piattaforma per sviluppare la migliore infrastruttura IT che il cliente necessita.
Fondata nell'ottobre del 1998 da Richard Yoo, Dirk Elmendorf e Patrick Condon, ha la propria sede a Windcrest, nello stato di San Antonio (USA).

- ***Confidentiality:*** *buona.*

  Rackspace specifica, all'interno dei propri “Terms & Conditions” contrattuali, che non condividerà alcun dato di proprietà dei clienti con terzi, se non dopo loro esplicita autorizzazione (eccetto nel caso in cui fossero richiesti dalla legge o siano fondamentali per tutelare la sicurezza e l'immagine sua e/o quella della propria clientela; in tali situazioni il provider diffonderà i dati del cliente dopo aver, comunque, provveduto ad avvisarlo tempestivamente).

  Se tale carattere confidenziale “venisse meno”, essa provvederà ad indennizzare il cliente tramite rimborso delle quote versate per l'utilizzo del servizio offerto.

- ***Integrity:*** *ottima.*

  Rackspace specifica, all'interno dei propri “Terms & Conditions” contrattuali, che l'integrità dei dati del cliente verrà garantita, qualora esso abbia proceduto al pagamento di specifici servizi di back-up addizionali (se tale integrità non venisse rispettata, il provider provvederà ad indennizzare il cliente tramite

rimborso delle quote versate per l'utilizzo del servizio offerto).

- ***Availability:*** *ottima.*

  Rackspace specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si ritiene responsabile per l'effettiva fornitura dei suoi servizi secondo i precetti indicati in essi; in caso di eventuali discordanze, provvederà ad indennizzare il cliente tramite rimborso delle quote versate, con il fine di fronteggiare sue eventuali perdite/danni derivanti dal malfunzionamento del servizio. Nello specifico, ad esempio, Rackspace garantisce l'operatività costante dei propri servizi (esclusi i preventivati e periodici intervalli per la manutenzione) e per ogni 30 minuti di eventuale inattività, rimborserà al cliente il 5% del totale che esso versa mensilmente per l'utilizzo dei servizi (fino a raggiungere, eventualmente, il 100% dell'esborso).

  Per ciò che riguarda le variazioni ai termini contrattuali (che possono incidere direttamente sull'availability), indica che, nel caso in cui vengano fatte, provvederà ad aggiornare i T&C sul proprio sito web e, da quel momento, tali modifiche diverranno effettive; il continuo utilizzo del servizio da parte del cliente rappresenterà un tacito assenso alle nuove condizioni derivanti dal cambiamento.

  Rackspace, inoltre, si riserva il diritto di poter modificare, sospendere o interrompere la fornitura del servizio offerto (o una parte di esso) nel caso di condotta illegale o non in linea con i T&C del contratto che regolano l'utilizzo

del servizio stesso.

Infine la preservazione dei dati é costantemente garantita, qualora il cliente abbia proceduto, anche in questo caso, al pagamento di specifici servizi di back-up addizionali.

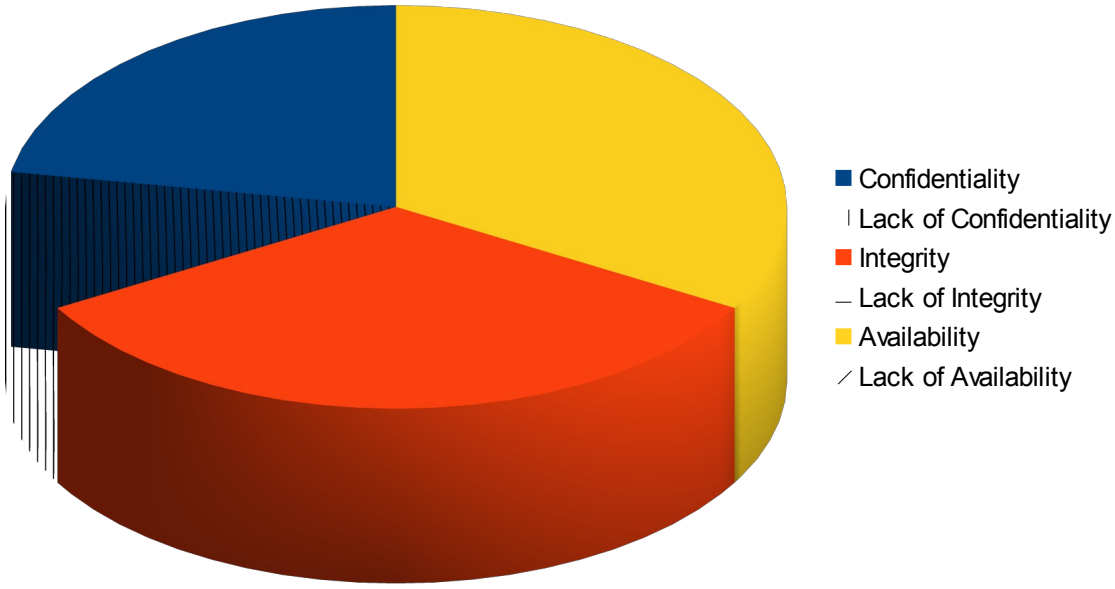

Grafico 4.9: La confidentiality, l'integrity e l'availability nei T&C di Rackspace.

4.2.10 Salesforce.com

Salesforce.com é un'azienda caratterizzata da un'architettura multitenant che consente di usufruire di svariati servizi SaaS per la gestione aziendale (come, ad esempio, quelli per monitorare le vendite) tramite un browser.

Fondata nel 1999 da Marc Benioff, Parker Harris, Dave Moellenhoff e Frank Dominguez, ha, attualmente, la propria sede a San Francisco, nello stato della California (USA).

- ***Confidentiality:*** *buona.*

  Salesforce.com specifica, all'interno dei propri "Terms & Conditions" contrattuali, che non condividerà alcun dato di proprietà dei clienti con terzi, se non dopo loro esplicita autorizzazione (eccetto nel caso in cui fossero richiesti dalla legge o siano necessari per portare a termine l'offerta del servizio/prevenire problemi tecnici allo stesso; in tali situazioni il provider diffonderà i dati del cliente dopo aver, però, provveduto ad avvisarlo tempestivamente).

  Se ritenuta colpevole dalla legge per l'accesso a tali informazioni da parte di soggetti non autorizzati, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare ciò che il cliente ha versato nei 12 mesi precedenti la domanda di indennizzo.

- ***Integrity:*** *sufficiente.*

  Salesforce.com specifica, all'interno dei propri "Terms & Conditions" contrattuali, che adotterà misure all'avanguardia per preservare l'integrità dei dati. Tuttavia non fornisce alcuna garanzia sulla riuscita di tali misure e, ove permesso dalla legge, declina ogni responsabilità derivante da perdite/danni ragionevolmente prevedibili, causati al cliente dall'alterazione/manomissione dei suoi dati da parte di terzi non autorizzati.

  Nel caso in cui Salesforce.com venisse dichiarata colpevole dalla legge, la sua responsabilità si limiterà, comunque, ad un rimborso di una quota che non potrà mai superare ciò che il cliente ha versato nei 12 mesi precedenti la domanda di indennizzo.

- ***Availability:*** *ottima.*

  Salesforce.com specifica, all'interno dei propri "Terms & Conditions" contrattuali, che si impegna a garantire l'offerta dei servizi richiesti secondo i dettami indicati in essi; se ciò non dovesse avvenire, provvederà ad indennizzare il cliente tramite rimborso delle quote versate (fino ad un tetto massimo equivalente a ciò che quest'ultimo ha versato nei 12 mesi precedenti per l'utilizzo dei servizi del provider), con il fine di fronteggiare sue eventuali perdite/danni derivanti dal malfunzionamento del servizio stesso.

  Per ciò che riguarda le variazioni ai termini contrattuali (che possono incidere direttamente sull'availability), indica che sono consentite e divengono effettive

solamente se in forma scritta e firmate in calce sia dal provider, sia dal cliente. Se, però, il cliente non rispettasse uno o più accordi contrattuali e perseverasse nel comportamento doloso per i 30 giorni conseguenti l'avviso di “condotta non regolamentare” ricevuto dal provider, Salesforce.com potrà terminare il servizio istantaneamente e avrà il diritto di trattenere (se già pagate) o di pretendere (se ancora da pagare) le somme dovute dal cliente dal momento in cui recede, a quando tale servizio avrebbe dovuto terminare secondo contratto. Inoltre se prima di 30 giorni dalla scadenza della collaborazione il cliente non affermasse di non volere continuare il rapporto, il rinnovo dello stesso avverrà automaticamente.

Infine al termine della collaborazione Salesforce.com concederà 30 giorni al cliente per recuperare i propri dati; una volta trascorso tale periodo, però, se la conservazione non fosse imposta dall'esterno per motivi legali, il provider procederà alla loro completa cancellazione.

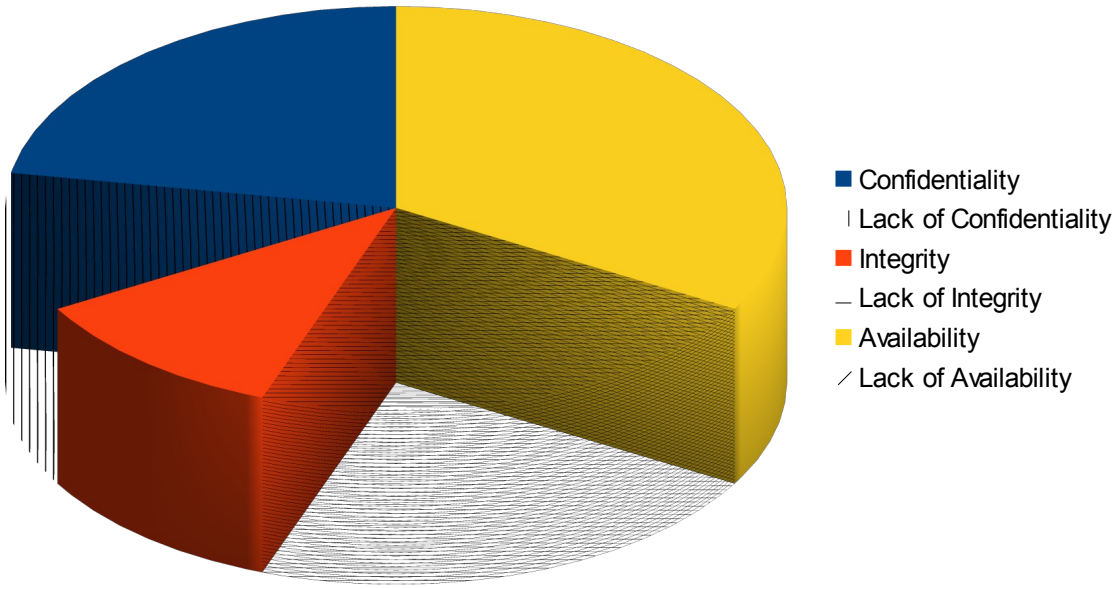

Grafico 4.10: La confidentiality, l'integrity e l'availability nei T&C di Salesforce.com.

4.2.11 Rappresentazione sommaria dei risultati ottenuti

Dopo aver analizzato, ad uno ad uno, i vari provider, ora procediamo ad una rappresentazione grafica sommaria che ne permetta un vicendevole confronto in termini di “Confidentiality”, “Integrity” e “Availability”.

Si é deciso di assegnare arbitrariamente i seguenti valori, dipendenti dalla qualità dei tre elementi sopra citati:

- ➔ Servizio *inadeguato* = “0”
- ➔ Servizio *sufficiente* = “1”
- ➔ Servizio *buono* = “2”
- ➔ Servizio *ottimo* = “3”

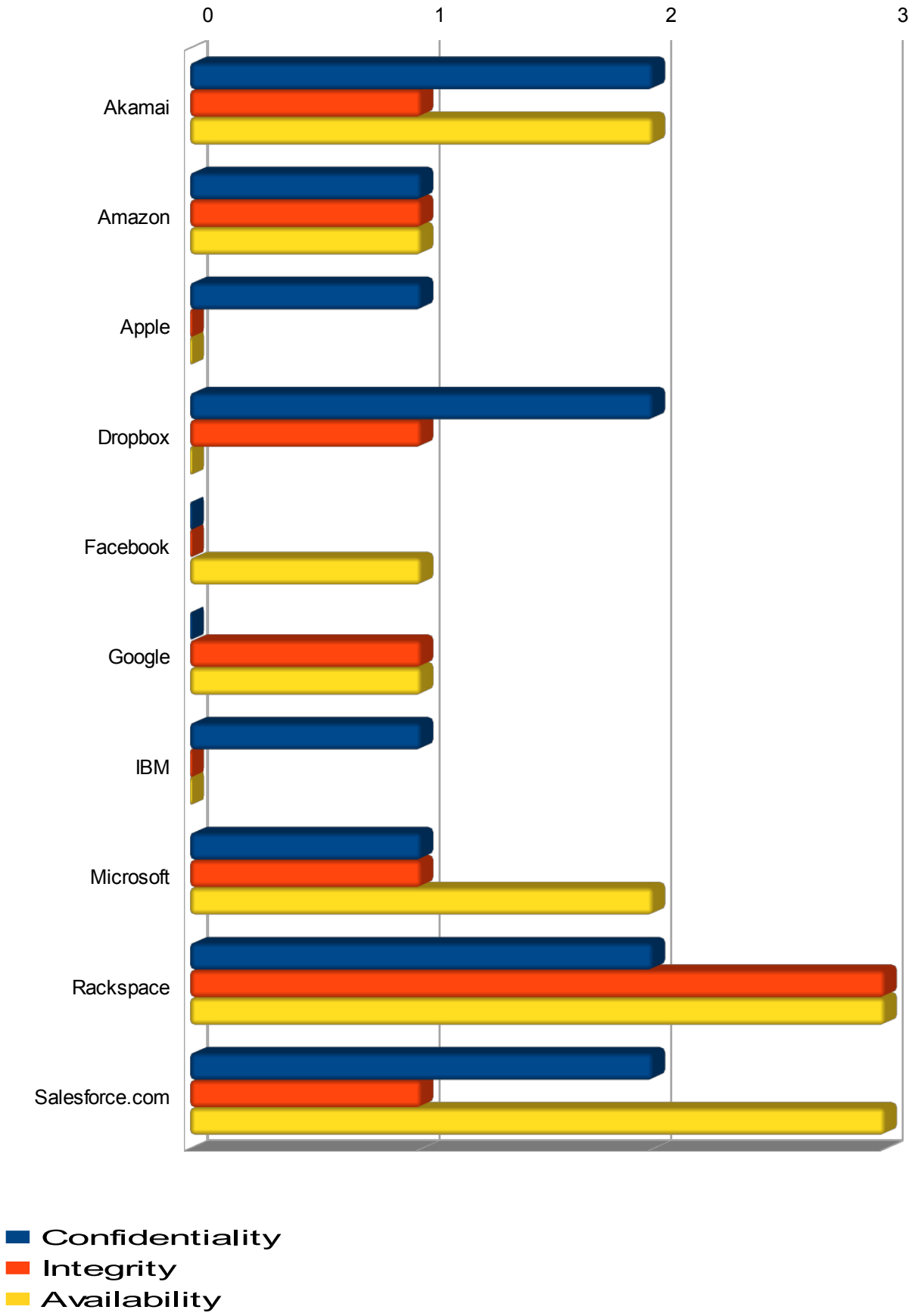

Grafico 4.11: La confidentiality, l'integrity e l'availability nei T&C di 10 tra i cloud provider più importanti su scala mondiale.

4.3 Le minacce alla sicurezza dei dati e le misure per contrastarle

Nell'ambito del cloud computing, come appena visto, la tematica della sicurezza dei dati del cliente assume un'importanza primaria; ciò é conseguenza del fatto che il cliente stesso, nell'affidarsi a questo tipo di servizio, condivide con un terzo (il fornitore del servizio stesso) un discreto ammontare di informazioni solitamente gestite internamente all'azienda.

Quello che rende ancora adesso molti manager riluttanti all'idea di adottare soluzioni cloud per la propria azienda, é proprio la paura che deriva dalla condivisione di dati sensibili. Per dissipare tali timori, i principi riguardanti la sicurezza e la privacy garantite dal provider devono essere costruiti su basi solide.

4.3.1 Gli attacchi DDoS

Cosa ha portato la maggior parte delle aziende a trasferire la propria e-mail all'interno di piattaforme cloud, avvicinandosi, così, per la prima volta, a questo tipo di servizi? Senza dubbio, principalmente, l'intenzione di difendersi dai cosiddetti attacchi “DDoS” (Distributed denial-of-service).

Gli attacchi DDoS si servono di un insieme di macchine chiamate “zombies”, che sono programmate per compiere azioni in simbiosi finalizzate a penetrare un server o un network con fini destabilizzanti.

Tali attacchi possono avere l'effetto di intasare il network bersagliato con una mole

così elevata di traffico fittizio, da impedire il funzionamento dell'intero sistema recando, di conseguenza, un danno agli utenti autorizzati ad accedervi e che hanno bisogno di servirsene.

Si tratta di attacchi semplici da attuare, ma complicati da fronteggiare. Considerando che la maniera più diffusa (e forse unica) di difendersi é quella di dotarsi di una “internet pipe” che possegga una dose talmente elevata di spazio al suo interno, tale da rendere ogni attacco di questo tipo infruttuoso, la soluzione-cloud computing sembra la più naturale da adottare.

Una “pipe” di una decina di gigabyte rappresenta, infatti, un costo spesso proibitivo per un'azienda e, al contempo, rimarrebbe di gran lunga sottoutilizzata, andando a costituire un effettivo spreco di denaro.

Se, invece, il costo di una “pipe” delle predette dimensioni venisse suddiviso tra più soggetti, come avviene, effettivamente, nelle piattaforme cloud, l'ammontare da spendere diverrebbe accessibile alla gran parte delle imprese e permetterebbe, quindi, di avere a disposizione ciò che serve per operare in un contesto più sicuro.

E' stata principalmente questa considerazione che ha spinto, come anticipato ad inizio paragrafo, la maggior parte delle aziende a trasferire la propria e-mail all'interno di ambienti cloud, consentendo, in molti casi, anche di ridurre i problemi di sovraccarico all'interno del normale funzionamento del network aziendale.

Va aggiunto, poi, che una scelta simile porta anche a beneficiare dei sistemi di sicurezza e controllo all'avanguardia dei cloud provider, che consentono di “filtrare” l'insieme di messaggi ricevuti quotidianamente, eliminando ogni forma di “spam” o

virus nascosti tra l'abituale corrispondenza telematica. (-Dragos Marian Mangiuc, "*Security issues of cloud based services"*, Review of international comparative management, 2012-)

Se, in origine, le piattaforme cloud hanno rappresentato una via di uscita ai potenziali problemi di un attacco di tipo DDoS, ultimamente, però, si stanno dimostrando anche preziose alleate per la loro propagazione. Le forze dell'ordine stanno riuscendo, infatti, a debellare i tipici attacchi DDoS, risalendo all'origine degli stessi e, quindi, individuando i cosiddetti "zombies" e chi li manovra, ma la stessa cosa non si può dire per le offensive che partono da una piattaforma cloud.

La nuova tendenza, infatti, é quella di sferrare attacchi con carte di credito rubate o contraffatte, tramite cui accedere temporaneamente ad un servizio IaaS, procedere nell'intento malevolo e, poi, dopo pochi minuti, terminare il pagamento del servizio e far perdere le proprie tracce.

Se, quindi, i DDoS rappresentano, raramente, una seria minaccia per i servizi cloud, (grazie, come visto in precedenza, all'elasticità di questi ultimi che permette alla struttura di riferimento di ampliare la capacità a disposizione a seconda del traffico presente), allo stesso modo, proprio grazie al cloud (e nello specifico alla sua caratteristica "paghi ciò che usi"), coloro che li "sferrano" hanno trovato un efficace stratagemma per non venire facilmente rintracciati.

4.3.2 L'encryption dei dati

L' “encryption”, definibile come protezione dei dati tramite apposito codice identificativo, é nata per far fronte ai timori delle imprese propense a “entrare nel cloud computing”.

Una volta deciso di usufruire di questo meccanismo di difesa, anche nel caso in cui soggetti non autorizzati riuscissero a fare breccia all'interno dei sistemi di sicurezza del provider, se non provvisti della “chiave di lettura” per avere accesso alle informazioni non sarebbero in grado di ottenere alcun beneficio dalla loro azione criminale; i dati obiettivo della loro intrusione rimarrebbero, infatti, illeggibili.

Se, poi, l'impresa che decidesse di adottare soluzioni cloud, non avesse piena fiducia nel provider (o le informazioni da condividere fossero di carattere confidenziale troppo elevato), potrebbe farsi essa stessa carico di procedere all' ”encryption”.

Così facendo i dati criptati raggiungerebbero il provider già “nascosti” e neppure quest'ultimo potrebbe avere la possibilità di visionarli. (-Mark D. Ryan, *“Cloud computing privacy concerns on our doorstep”*, Communications of the ACM, 2011-)

In ogni caso, però, gli schemi e le procedure che caratterizzano la crittografia dei dati vanno delineati e testati da specialisti appositi; tale premura evita il rischio che, in caso di incidenti, i dati criptati vadano persi, divenendo inutilizzabili per chiunque ne voglia avere accesso (compresa l'impresa proprietaria degli stessi).

Conclusioni

All'interno di questa tesi, dopo aver provveduto a presentare il concetto di cloud computing e a delineare le varie sfaccettature che caratterizzano la relazione provider-cliente, ci si é concentrati sugli aspetti concernenti la sicurezza presenti nel contratto, vero obiettivo dell'intero lavoro.

Per fare ciò sono stati presi in considerazione 10 provider tra i più rinomati sulla scena internazionale in termini di servizi cloud (Akamai, Amazon, Apple, Dropbox, Facebook, Google, IBM, Microsoft, Rackspace e Salesforce.com) e, analizzando nel dettaglio i loro "T&C" (Terms & Conditions) contrattuali, si é definito il livello di sicurezza fornito da ciascuno di essi, suddividendolo lungo tre dimensioni, tutte riguardanti, direttamente o indirettamente, la gestione dei dati del cliente da parte del provider; "*confidentiality*", "*integrity*", "*availability*".

Il panorama che ne consegue, illustrato dettagliatamente nel "Grafico 4.11", é il seguente; i migliori valori sono quelli ottenuti da Akamai, Rackspace e Salesforce.com, mentre i peggiori sono quelli riscontrati in Apple, Facebook, Google e IBM.

Risultati di questo genere sono, a mio parere, per nulla sorprendenti e ci portano a

trarre delle precise conclusioni.

Non é un caso, infatti, che le migliori performance in termini di sicurezza si verifichino nel caso dei tre provider dall'immagine meno prestigiosa/conosciuta tra la gente.

Per Apple, Facebook, Google e IBM qualsiasi genere di garanzia in termini di confidentiality, integrity e availability dei dati della clientela, presenti all'interno delle proprie piattaforme cloud, andrebbe a sfociare in una potenziale ricaduta economica maggiore di quella che deriva dalla perdita di clienti non soddisfatti dei requisiti di sicurezza offerti e che, quindi, si rivolgono ad un altro provider. Il loro bacino di utenza é troppo ampio per essere assicurato contro qualsiasi attacco esterno o malfunzionamento del servizio che porti alla modifica/perdita di alcuni dati e, contemporaneamente, la forza del loro “brand”, spesso, funge essa stessa da garanzia per il consumatore; perciò essi si limitano a promettere il loro massimo impegno e l'uso di strumenti all'avanguardia con fini di “security”, ma non si spingono oltre declinando ogni responsabilità in merito alla riuscita effettiva dei provvedimenti presi.

Allo stesso tempo confidano nella superficialità della clientela che, effettivamente, molto raramente si premura di analizzare i “T&C” alla base del contratto che regola il servizio offerto, accontentandosi, per pigrizia, di verificare che esso risponda alle esigenze richieste e ricercate.

Il discorso differisce marcatamente per ciò che riguarda provider come Akamai, Rackspace e Salesforce.com; in questi casi essi partono da una posizione iniziale di

chiaro svantaggio rispetto agli altri presi in considerazione, incarnanti un marchio diffuso, radicato e ultraconosciuto sul mercato[22].

Ciò non vuole assolutamente dire che i servizi da loro presentati siano di livello inferiore, ma che per espandere il proprio insieme di utilizzatori (sottraendone, anche, alla concorrenza), debbano concentrarsi sulla proposta di un prodotto differenziato, che sia in grado di guadagnarsi un segmento di mercato caratterizzato da bisogni non adeguatamente soddisfatti o non curati del tutto; da qui l'idea di offrire maggiori garanzie sotto forma di rispetto del carattere confidenziale dei dati, di salvaguardia dalla modifica degli stessi da parte di soggetti non autorizzati e di loro costante disponibilità in caso si voglia averne accesso (in simultanea con la promessa di un servizio sempre funzionante).

22 Si intende "*mercato*" in generale, non solamente quello riguardante il settore cloud.

Bibliografia

- Alali Fatima A., Chia-Lun Yeh, (2012), *Cloud computing: overview and risk analysis*, Journal of Information Systems, Vol. 26, Issue 2, pagg. 13-33.
- Armbrust Michael, Fox Armando, Griffith Rean, Joseph Anthony D., Katz Randy, Konwinski Andy, Lee Gunho, Patterson David, Rabkin Ariel, Stoica Ion, Zaharia Matei, (2010) *A view of cloud computing*, Communications of the ACM, Vol. 53, Issue 4, pagg. 50-58.
- Bidgoli Hossein, (2011), *Successful introduction of cloud computing into your organization: a six-step conceptual model*, Journal of International Technology & Information Management, Vol. 20, Issue 1/2, pagg. 21-38.
- Bloomberg Jason, (2013), *Wiley CIO: agile architecture revolution: how cloud computing, REST-based SOA and mobile computing are changing enterprise IT*, Wiley, Somerset (USA).
- Blowers Helene, (2012), *Considering the cloud and the greater computing atmosphere*, Computers in libraries, Vol. 32, Issue 4, pagg. 29-31.

- Bradshaw Simon, Millard Christopher, Walden Ian, (2011), *Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services*, International Journal of Law and Information Technology, Vol. 19, No. 3.
- Budriene Daiva, Zalieckaite Laima, (2012), *Cloud computing application in small and medium-sized enterprises*, Issues of Business & Law, Vol. 4, pagg. 99-130.
- Burton Daniel, (2012), *What cloud computing means for government*, Government news, Vol. 32, Issue 1, pagg. 16-17.
- Choi Eunjeong, (2013), *How cloud computing is revolutionizing the future*, SERI Quarterly, Vol. 6, Issue 3, pagg. 104-109.
- Christauskas Ceslovas, Miseviciene Regina, (2012), *Cloud computing based accounting for small to medium sized business*, Engineering Economics, Vol. 23, Issue 1, pagg. 14-21.
- Cohen Reuven, (2012), *The past, the present and the future of cloud computing*, Intel Technology Journal, Vol.16, Issue 4, pagg. 20-24.
- Cusumano Michael, (2010), *Technology strategy and management: cloud computing and SaaS as new computing platforms*, Communications of the ACM, Vol. 53, Issue 4, pagg. 27-29.
- Durkee Dave, (2010), *Why cloud computing will never be free*, Communications of the ACM, Vol. 53, Issue 5, pagg. 62-69.

- Dutta Amab, Guo Chao Alex Peng, Choudhary Alok, (2013), *Risks in enterprise cloud computing: the perspective of IT experts*, Journal of Computer Information Systems, Vol. 53, Issue 4, pagg. 39-48.
- Filev Dimitar, Lu Jianbo, Hrovat Davor, (2013), *Future mobility: integrating vehicle control with cloud computing*, Mechanical Engineering, Vol. 135, Issue 3, Special Section pagg. 18-24.
- Garrison Gary, Kim Sanghyun, Wakefield Robin L., (2012), *Success factors for deploying cloud computing*, Communications of the ACM, Vol. 55, Issue 9, pagg. 62-68.
- Gold Joshua, (2012), *Protection in the cloud: risk management and insurance for cloud computing*, Journal of Internet Law, Vol. 15, Issue 12, pagg. 1-28.
- Greengard Samuel, (2010), *Cloud computing and developing nations*, Communications of the ACM, Vol. 53, Issue 5, pagg. 18-20.
- Helland Pat, (2013), *Condos and clouds*, Communications of the ACM, Vol. 56, Issue 1, pagg. 50-59.
- Hugos Michael, Hulitzky Derek, (2010), *Business in the cloud: what every business needs to know about cloud computing*, Wiley, Hoboken (USA).
- Indranil Bose, (2012), *Cloud computing and its impact on corporate HR practices*, Advances in Management, Vol. 5, Issue 10, pagg. 68-69.
- Juels Ari, Oprea Alina, (2013), *New approaches to security and availability for cloud data*, Communications of the ACM, Vol. 56, Issue 2, pagg. 64-73.

- Kalyvas James R., Overly Michael R., Karlyn Matthew A., (2013), *Cloud computing: a practical framework for managing cloud computing*, Intellectual Property & Technology Law Journal, Vol. 25, Issue 3, pagg. 7-18.
- Katzan Jr. Harry, (2010), *On an ontological view of cloud computing*, Journal of Service Science, Vol. 3, Issue 1, pagg. 1-6.
- Kshetri Nir, (2011), *Cloud computing in the global south : drivers, effects and policy measures*, Third World Quarterly, Vol. 32, Issue 6, pagg. 997-1014.
- Ling Zhang, Wenlin Gu, (2013), *The simple analysis of impact on financial outsourcing because of the rising of cloud accounting*, Asian Journal of Business Management, Vol.5, Issue 1, pagg. 140-143.
- Mangiuc Dragos-Marian, (2012), *Security issues of cloud based services – a guide for managers*, Review of International Comparative Management, Vol. 13, Issue 3, pagg. 468-477.
- Marks Eric A., Lozano Bob, (2010), *Executive's guide to cloud computing*, Wiley, Hoboken (USA).
- Maughan Alistair, (2013), *Europe offers incentives to cloud computing growth*, Intellectual Property & Technology Law Journal, Vol. 25, Issue 2, pagg. 14-19.
- McDonald Kevin T., (2010), *Above the clouds: managing risk in the world of cloud computing*, IT Governance, Cambs (GBR).
- Mell Peter, Grance Tim, (2010), *The NIST definition of cloud computing*, Communications of the ACM, Vol. 53, Issue 6, pag. 50.

- Muller Hunter, (2011), *On top of the cloud: how CIOs leverage new technologies to drive change and build value across the enterprise*, Wiley, Hoboken (USA).
- Ross Peter, (2011), *How to keep your head above the clouds: changing ICT worker skill sets in a cloud computing environment*, Employment Relations Record, Vol. 11, Issue 1, pagg. 62-74.
- Rouse Margaret, (2013), *Confidentiality, integrity and availability*, whatis.techtarget.com.
- Ryan Mark D., (2011), *Cloud computing privacy concerns on our doorstep*, Communications of the ACM, Vol. 54, Issue 1, pagg. 36-38.
- Schwartz Paul M., (2013), *Information privacy in the cloud*, University of Pennsylvania Law Review, Vol. 161, Issue 6, pagg. 1623-1662.
- Sood Sandeep K., (2012), *A combined approach to ensure data security in cloud computing*, Journal of Network and Computer Applications, Vol. 35, Issue 6, pagg. 1831-1838.
- Sotola Rene, (2011), *Billing in the cloud: the missing link for cloud providers*, Journal of Telecommunications management, Vol. 3, Issue 4, pagg. 313-320.
- Srivastava Kamal, Kumar Atul, (2011), *A new approach of cloud: computing infrastructure on demand*, Trends in Information Management, Vol. 7, Issue 2, pagg. 145-153.

- Sunyaev Ali, Schneider Stephan, (2013), *Cloud service certification*, Communications of the ACM, Vol. 56, Issue 2, pagg. 33-36.
- Tsai Brian J., Shen John, (2012), *Securities operations: in-house or in the cloud*, Journal of Securities Operations & Custody, Vol. 5, Issue 2, pagg. 110-117.
- Vakil Farok, Lu Victor, Russakoff Andrew, (2013), *Recent developments in cloud computing and high speed connections for business paractices*, Review of Business, Vol. 33, Issue 1, pagg. 111-118.
- Von Solms R., Viljoen M., (2012), *Cloud computing service value: a message to the board*, South African Journal of Business Management, Vol. 43, Issue 4, pagg. 73-81.
- Waxer Nathan, Ninan David, Ma Alfred, Dominguez Norma, (2013), *Continuous quality monitoring through analytics and cloud computing*, Physician Executive, Vol. 39, Issue 5, pagg. 36-39.
- Waxer Nathan, Ninan David, Ma Alfred, Dominguez Norma, (2013), *How cloud computing and social media are changing the face of health care*, Physician Executive, Vol. 39, Issue 2, pagg. 58-62.
- Williams Mark I., (2010), *A quick start guide to cloud computing: moving your business into the cloud*, Kogan Page, (GBR).

- Yeh Ching-Wen, (2012), *Cloud computing and human resources in the knowledge era*, Human Systems Management, Vol. 31, Issue 3/4, pagg. 165-175.
- Yoo Christopher, (2011), *Cloud computing: architectural and policy implications*, Review of Industrial Organization, Vol. 38, Issue 4, pagg. 405-421.
- Zota Razvan Daniel, Fratila Lucian-Alexandru, (2013), *Cloud standardization: consistent business processes and information*, Informatica Economica, Vol. 17, Issue 3, pagg. 137-147.