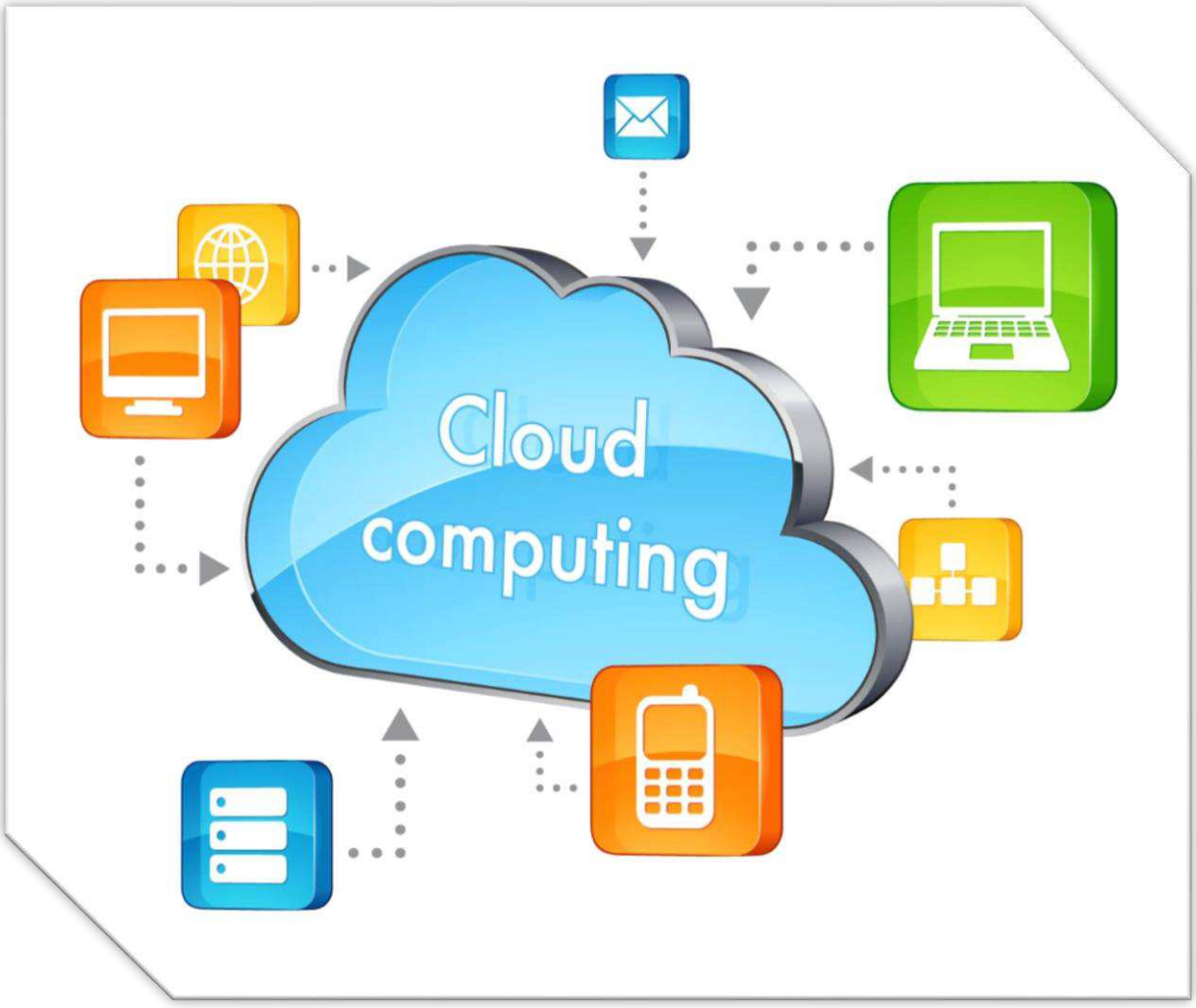
eBook

Digital & Law Department

Le 5 W del cloud computing

redatto dall'Avv. Sarah Ungaro

con la supervisione dell'Avv. Andrea Lisi



Sommario

Testo aggiornato al 29/04/2014

1. WHAT? - Cos'è il cloud computing

Il *cloud computing*, inteso come modello flessibile ed economico di fornitura di servizi ICT, rappresenta non solo uno strumento di risparmio e razionalizzazione delle risorse informatiche ma anche - e soprattutto - un nuovo metodo per progettare, realizzare e gestire i sistemi informativi delle aziende e delle pubbliche amministrazioni.

La sempre crescente diffusione dei sistemi cloud costituisce, dunque, una "*forza di distruzione creatrice*", che induce a organizzare in modo più efficiente ed economico la gestione di risorse, dati e informazioni.

Dalle pubbliche amministrazioni alle imprese fino ai singoli utenti, tutti possono beneficiare di questa rivoluzione: non ci sarà più bisogno di memorizzare i dati localmente sugli hard disk e di fare periodici backup, ma sarà possibile accedere on line da qualsiasi client alla potenza di elaborazione, alle piattaforme, ai servizi, ai software e ai documenti immagazzinati sulla nuvola virtuale gestita dal *cloud service provider*: ciò a tutto vantaggio della praticità ed economicità dei processi documentali e produttivi.

Con particolare attenzione verso le pubbliche amministrazioni, il *cloud* permette di conseguire più agevolmente gli obiettivi di efficacia, efficienza, trasparenza, partecipazione, condivisione, cooperazione, interoperabilità e sicurezza nell'agire amministrativo.

Per tali motivi, l'utilizzo del *cloud* da parte della pubblica amministrazione è previsto nelle strategie ICT di molti Paesi. A livello UE si moltiplicano i riferimenti al *cloud computing* nei documenti strategici (Digital Agenda for Europe, EU Cloud Initiative, eGovernment Action Plan 2011 - 2015) e nei principali programmi (programma ISA, 7° programma quadro di ricerca, programma CIP – ICT PSP).

Anche in Italia, con l'art. 47 della legge n. 35/2012 (di conversione del D.L. n. 5/2012), sono state individuate una serie di misure da adottare per il perseguimento degli **obiettivi dell'Agenda digitale italiana**, tra le quali, alla lett. d), è espressamente menzionata la "*promozione della diffusione e del controllo di architetture di cloud computing per le attività e i servizi delle pubbliche amministrazioni*".

1.1 Ma precisamente, cos'è il cloud?

*"I sistemi cloud sono grandi contenitori di **risorse virtuali** di facile utilizzo e accesso (che mettono a disposizione vari software, ma anche l'hardware, le piattaforme di sviluppo e/o di servizio, la potenza di calcolo). Queste **infrastrutture informatiche** possono essere dinamicamente riconfigurate per adattarsi a un carico di lavoro variabile (scalabilità), consentendo anche un'utilizzazione ottimale delle risorse. Questo sistema è impiegato tipicamente secondo il modello pay-for-use nel quale tutto è garantito dal provider dell'infrastruttura tramite SLA personalizzati"*[1].

[1] Secondo la definizione dell'ACM Computer Communication Review , in "*A Break in the Clouds: Towards a Cloud Definition*", di L. M. Vaquero, L. Rodero-Merino, J. Caceres, M. Lindner, Vol. 39, N. 1, January 2009.

Secondo la definizione formulata dal **National Institute of Standards and Technology (NIST)**[2], nel *cloud* è possibile individuare modalità di fornitura diverse e modelli di servizio differenti.

Riguardo alle **modalità di fornitura dei servizi cloud**, occorre scegliere la soluzione più adatta alle esigenze dell'azienda o dell'ente interessato. In particolare, le valutazioni possibili possono articolarsi sulle modalità **IaaS** (**Infrastructure as a Service**, attraverso le quali, secondo un modello *pay per use*, gli strumenti hardware e software di base come reti, capacità di elaborazione, sistemi operativi, risorse di memorie di massa, applicazioni e servizi, sono messi a disposizione dell'ente mediante server virtuali), **SaaS** (**Software as a Service**, modalità spesso impiegata per le applicazioni che vengono comunemente utilizzate negli uffici in modalità web, come l'elaborazione di fogli di calcolo o di testi, la gestione del protocollo e delle regole per l'accesso informatico ai documenti, la rubrica dei contatti e dei calendari condivisi, ma anche alcuni dei più avanzati servizi di posta elettronica) o **PaaS** (**Platform as a Service**, ossia una tipologia di servizio rivolto a operatori di mercato che lo utilizzano per sviluppare e ospitare soluzioni applicative proprie, come quelle per la gestione finanziaria, della contabilità o della logistica, per assolvere esigenze interne, oppure per fornire a loro volta servizi a terzi).

Con specifico riferimento invece ai **modelli di servizio**, esistono *cloud pubblici*, *privati* e *ibridi*.

Un modello di ***public cloud*** (o anche *cloud esterno*) è quello in cui i *cloud service provider* e l'ente destinatario del servizio non appartengono alla stessa struttura organizzativa, per cui le infrastrutture cloud sono rese accessibili a una platea indistinta di potenziali utenti.

Nel ***private cloud*** (noto anche come *cloud interno*), i fornitori e gli utilizzatori di un servizio appartengono invece alla medesima organizzazione.

È importante evidenziare che è possibile optare per un modello di *cloud privato* per avere un maggiore controllo dei dati: nel *cloud interno*, infatti, questi rimangono presso le strutture organizzative su cui l'ente ha pieno ed esclusivo controllo. Adottando questo sistema, il patrimonio di dati personali e sensibili - o addirittura ultrasensibili - dell'ente può essere trattato direttamente e unicamente all'interno dell'organizzazione stessa.

L'implementazione di un sistema di *cloud privato*, tuttavia, comporta che i relativi servizi siano forniti mediante risorse dedicate esclusivamente all'organizzazione dell'azienda, con un inevitabile aumento dei costi.

Per ovviare a tale inconveniente, dunque, molti enti o aziende decidono di ricorrere a un ulteriore modello di servizio rappresentato dal ***cloud ibrido***. In questo modo è possibile demandare a un sistema di *cloud pubblico* servizi o applicazioni che coinvolgono il trattamento di dati non personali, magari in modalità aggregata, o comunque non sensibili, mentre determinati processi che interessano tipologie di dati che esigono misure di sicurezza rafforzate, vengono gestiti mediante un modello di *cloud privato*.

Nello specchietto che segue si riassumono le caratteristiche salienti delle diverse modalità:

[2] Si veda "*Cloud computing Synopsis and Recommendations*. Recommendations of the National Institute of Standards and Technology - NIST - Special Publication 800-146, May 2012", a cura di L. Badger, T. Grance, R. Patt-Corner, J. Voas.

MODELLI DI SERVIZIO DEL CLOUD COMPUTING		
IAAS Infrastructure As A Service Infrastruttura con capacità computazionale, di memorizzazione, e di rete, sulla quale è possibile installare ed eseguire il software necessario all'utente	**PAAS** Platform As A Service Interfaccia di programmazione (API) messa a disposizione dal fornitore con la quale l'utente può scrivere applicazioni che interagiscono con il servizio	**SAAS** Software As A Service Applicazione software che può essere utilizzata su richiesta. Il fornitore del servizio installa l'applicazione nei propri data center e fornisce agli utenti un'interfaccia per utilizzarla

MODELLI DI FRUIZIONE DEL CLOUD COMPUTING			
Public Cloud L'infrastruttura su cui sono installati i servizi cloud è offerta dal fornitore che mette a disposizione dei propri utenti/clienti la potenza di calcolo e/o di memorizzazione dei suoi data center	Private Cloud L'infrastruttura su cui sono installati i servizi cloud è di esclusiva titolarità dell'utente che ha il pieno controllo delle macchine sulle quali vengono conservati i dati e vengono eseguiti i suoi processi	Community Cloud L'infrastruttura su cui sono installati i servizi cloud è condivisa da un insieme di soggetti, aziende, organizzazioni, ecc. che condividono uno scopo comune e che hanno le stesse esigenze	Hybrid Cloud Combinazione del modello pubblico e di quello privato, ovvero modello in cui l'utente utilizza risorse sia del suo cloud privato che di un cloud pubblico

2. WHY? - Perché implementare il cloud

Nelle strutture che gestiscono imponenti quantità di dati l'implementazione di sistemi cloud consente di **risparmiare i costi** di acquisito delle licenze software, di nuovi hardware e soprattutto di tenuta dei tradizionali data center, ma al contempo permette anche di **sfruttare una potenza di calcolo scalabile**, avvalendosi di una serie di opzioni che possono consentire una maggiore flessibilità nella gestione dei processi documentali e favorire un incremento della qualità dei servizi resi.

I sistemi cloud, inoltre, possono offrire come servizio anche **uno spazio di storage dinamicamente calibrato**.

In questo contesto, la virtualizzazione dello storage presenta una serie di vantaggi: l'idea fondamentale è quella di slegare l'archiviazione dei dati dal tradizionale sistema di data center, che costituisce un modello statico di digital preservation. Tale scelta è adottata anche al fine di evitare il rischio che calamità naturali o attacchi informatici possano compromettere il funzionamento di alcuni data center.

Le applicazioni cloud, invece, utilizzano questi archivi per soddisfare in modo dinamico le diverse esigenze di **digital preservation**.

Per quanto riguarda i trasferimenti di dati, viene utilizzata solitamente un'apposita Storage Area Network (SAN) o una rete aziendale locale (LAN), mentre un ulteriore livello di gestione virtuale dei dati si inserisce tra i client e le varie risorse di memoria, in modo che la rappresentazione informatica degli stessi dati venga svincolata dalla sua localizzazione fisica.

Questo processo presenta una serie di vantaggi per quanto riguarda la gestione dei dati e la scalabilità delle risorse impiegate: tale gestione centralizzata, infatti, consente anche di implementare a un costo inferiore i diversi sistemi di storage distribuiti.

Inoltre, anche mediante i servizi cloud, le diverse categorie di dati oggetto di archiviazione possono essere organizzate in un sistema di digital preservation programmato in base a un criterio gerarchico. Ciò rende possibile implementare un sistema predisposto per la gestione del ciclo di vita delle differenti tipologie di dati, da quelli per cui si richiede una maggiore disponibilità di banda e dei maggiori livelli di sicurezza (trasmissione e archiviazione cifrate) a quelli per i quali è sufficiente un sistema più economico e quindi corrispondente a una qualità meno elevata di servizio.

Ulteriori vantaggi della digital preservation in cloud sono i sistemi distribuiti di ridondanza dei dati, che possono essere creati e gestiti al fine di evitare interruzioni del servizio in caso di malfunzionamenti, grazie alle creazione di copie degli stessi dati da allocare in data center diversi.

Tuttavia, **il profilo della sicurezza dei dati è sempre stato un aspetto critico dello storage IT**. In tal senso, la proliferazione di tecnologie di rete e protocolli, in combinazione con l'emergere del fenomeno del *cloud storage*, ha reso sempre più stringente l'esigenza di garantire la sicurezza di dati e informazioni.

È necessario evidenziare che il problema si pone soprattutto perché, mentre i contenuti di un documento cartaceo possono essere accessibili a una platea di soggetti tendenzialmente ristretta, al contrario **le operazioni di *cloud storage*** dei documenti digitali, se non c'è stata un'attenta considerazione dei fattori di rischio che le connotano, possono **rendere i dati coinvolti potenzialmente alla portata di tutti gli utenti del web**. Per questi motivi appare

indispensabile un'oculata analisi dei rischi e una conseguente pianificazione della gestione organizzativa dei dati.

2.1 E per le pubbliche amministrazioni?

Anche per le pubbliche amministrazioni oggi le parole d'ordine sono: utilizzare il *cloud computing* per risparmiare!

In verità, servirsi della "nuvola" nella pubblica amministrazione non deve significare solo adottare una nuova e più conveniente infrastruttura tecnologica, ma deve essere piuttosto una scelta consapevole verso una minore burocratizzazione dei processi decisionali e, quindi, una potenziale trasformazione delle modalità di interazione tra PA, cittadini e imprese, in direzione di una maggiore trasparenza e partecipazione e di un miglioramento dei servizi offerti. Prevedere l'implementazione dei sistemi cloud nella pubblica amministrazione, infatti, se da una parte può consentire l'immediato accesso a una potenza di calcolo graduabile e alla virtualizzazione dei servizi - anche di digital preservation - dall'altra parte comporta l'inevitabile **affidamento in capo ai *cloud provider* della responsabilità nella gestione di alcune tipologie di dati pubblici**. Ed è proprio per questa ragione che, in caso di esternalizzazione di questo tipo di servizi, occorre intervenire sia sul profilo organizzativo, sia su quello contrattuale, affinché l'introduzione del *cloud* nella PA abbia gli esiti auspicati, limitando i fattori di criticità relativi agli intrinseci caratteri di delocalizzazione e di anazionalità che connotano questa tecnologia.

Fatte queste doverose premesse, il *cloud computing*, nelle sue diverse applicazioni (IaaS/Paas/SaaS, privato/pubblico/di comunità/ibrido) rappresenta quindi una buona soluzione, sia per permettere **l'adeguamento delle singole pubbliche amministrazioni al dettato dell'art. 50-*bis* (continuità operativa e disaster recovery)**, sia per la risoluzione di alcune problematiche legate al mondo della digitalizzazione dei dati e documenti delle pubbliche amministrazioni che, alla luce dell'Agenda digitale - e ancor prima del Codice dell'Amministrazione Digitale - sono obbligate a rendere **accessibili ai cittadini i propri servizi in modalità telematica**, seppur molto spesso non dispongano di adeguate risorse hardware e software al loro interno.

Se il *cloud*, quindi, rappresenta una sicura risorsa per una maggiore efficienza nell'amministrazione dei servizi pubblici, le pubbliche amministrazioni dovrebbero valutare seriamente **la possibilità di gestire e conservare i propri documenti attraverso sistemi di conservazione basati su tecnologie cloud**.

Sempre più spesso, infatti, le PA si trovano a fare i conti con la necessità (oltre che il preciso obbligo normativo) di conservare i propri documenti informatici. Se fino ad oggi l'utilizzo del documento informatico è stato comunque molto limitato nella PA, con sempre maggiore incidenza specifiche norme impongono, al contrario, il suo utilizzo. Basti pensare all'effetto dirompente che la fatturazione elettronica avrà nei confronti di tutte le pubbliche amministrazioni sia centrali che locali. Con l'approvazione del Regolamento **di cui al DM 55/2013**, infatti, **potranno essere pagate esclusivamente le fatture emesse elettronicamente** e queste ultime, secondo il chiaro dettato **dell'art. 43 del CAD (nonché della legge 24 dicembre 2007, n. 244, che ha istituito l'obbligo di fatturazione elettronica per la PA), potranno essere conservate solamente in modalità digitale**.

Anche in questo specifico campo il *cloud* potrebbe rappresentare una vera e propria opportunità, che permette alle pubbliche amministrazioni di ottemperare al dettato normativo senza effettuare, sin da subito, ingenti investimenti in capitali e risorse umane e tecnologiche.

Sulla questione **anche l'Unione Europea sta accelerando i tempi**, ponendo come fulcro della propria Agenda Digitale la diffusione del *cloud computing*.

Al fine di agevolare lo sviluppo tecnologico conseguibile attraverso le infrastrutture cloud, infatti, è stato costituito il Comitato direttivo del nuovo partenariato europeo per il *cloud computing* (European Cloud Partnership - ECP), cha ha l'ambizioso obiettivo di avviare un processo di collaborazione tra pubbliche amministrazioni e imprese, per contribuire alla creazione di un mercato unico UE della nuvola informatica, conformemente alla strategia europea per il *cloud computing*.

In particolare, gli obiettivi fondamentali fissati dal Comitato direttivo dell'ECP (la cui principale missione consiste nel fornire consulenza strategica e nel definire orientamenti per eventuali nuove iniziative nell'ambito del partenariato) sono l'armonizzazione dell'offerta di servizi, lo sviluppo di partnership tra pubbliche amministrazioni ed enti privati, la definizione di linee guida per i contratti, lo stimolo di azioni di joint procurement, la valorizzazione delle best practice e la promozione dell'interoperabilità e della portabilità dei dati e dei servizi.

Nello specifico, l'European Cloud Partnership riunirà autorità pubbliche e consorzi privati, al fine di lanciare appalti pubblici pre-commerciali relativi a servizi di *cloud computing* per il settore pubblico. Lo stesso ente provvederà, poi, a definire anche i requisiti relativi agli appalti, requisiti che gli Stati membri e le autorità pubbliche applicheranno in tutta l'Unione Europea.

Per realizzare questo scopo l'ECP prevede un investimento iniziale di 10 milioni di euro che serviranno a creare una solida base comune per gli appalti cloud da parte degli enti pubblici di tutti i Paesi membri, sfruttando il potere d'acquisto di questi ultimi per modellare e indirizzare il crescente mercato europeo dei servizi informatici in *cloud*.

Inoltre, lo stesso comitato ha deciso di coadiuvare la Commissione europea nell'individuazione degli standard e dei sistemi di certificazione del *cloud computing*: ciò avverrà anche attraverso l'avvio di progetti pilota transnazionali e interoperabili, in ambiti strategici dell'attività pubblica ed economica.

3. WHO? - Ruoli e responsabilità

Preliminare all'analisi dei profili di responsabilità è la disamina dei ruoli e degli attori che possono intervenire nei modelli di servizio cloud .

Nello specifico, le figure di rilievo sono: il **cloud provider** (che acquisisce e gestisce le infrastrutture di elaborazione necessarie a fornire i servizi attraverso la rete e assicura l'esecuzione dei programmi che consentono i servizi), il **cloud consumer** (ossia l'utente o l'organizzazione che sottoscrive un contratto con il cloud provider), il **cloud auditor** (che è il soggetto che può eseguire un controllo indipendente sui servizi erogati da un cloud provider con il fine di esprimere un parere, ad esempio in merito alla sicurezza, all'impatto sulla privacy e al livello delle prestazioni), il **cloud broker** (il soggetto che gestisce l'impiego, le prestazioni e l'erogazione dei servizi cloud e cura le relazioni tra il cloud provider e il cloud consumer) e il **cloud carrier** (il quale agisce come un intermediario, fornendo la connettività e il trasporto di servizi cloud tra il cloud consumer e il cloud provider, nonché l'accesso al cloud consumer attraverso le reti e i dispositivi).

Inoltre, nel caso in cui siano i **dati di una pubblica amministrazione** a essere trasferiti in cloud, occorre considerare anche ulteriori risvolti, per esempio nella scelta tra i differenti modelli di servizio: tale valutazione non può non tenere in considerazione due aspetti fondamentali che andiamo ora ad approfondire.

Il primo riguarda la possibilità di trasferire all'esterno dell'ente i suoi archivi. Mentre, infatti, sono liberi i trasferimenti di parti dell'archivio corrente tra le sedi della pubblica amministrazione (art. 21, c.3 D.Lgs 42/2004), occorre **l'autorizzazione della Soprintendenza Archivistica per eventuali trasferimenti parziali o totali degli archivi di deposito o storici tra sedi dello stesso Ente e per trasferimenti di complessi organici di documentazione ad altre persone giuridiche (art. 21, c.1-e D.Lgs 42/2004)**. È il caso della cessione di documenti necessari per l'esercizio di competenze trasferite tra enti o dell'affidamento di servizi in "outsourcing". La violazione di tali obblighi è punita con la nullità degli atti giuridici (art. 164, c.1 D.Lgs 42/2004), con l'arresto da sei mesi a un anno e con l'ammenda da euro 775 a euro 38.734,50 (art. 169, c.1 D.Lgs 42/2004).

Ad eccezione, quindi, dei trasferimenti tra le diverse sedi dell'ente di documentazione che appartenga all'archivio corrente, l'esecuzione di opere e lavori di qualunque genere sull'archivio corrente, di deposito e storico dell'ente sono subordinati ad autorizzazione della Soprintendenza, che deve darla su progetto o almeno su "descrizione tecnica dell'intervento", con eventuali prescrizioni delle cautele necessarie (art. 21, commi 4 e 5, D.Lgs 42/2004).

Un secondo aspetto fondamentale da tenere presente è quello relativo al **diritto di accesso ai documenti conservati**, che dovrebbe essere sempre garantito. Si rammenta, infatti, che ai sensi della normativa sulla trasparenza amministrativa, i documenti dell'archivio corrente e di deposito, compresi gli atti interni, si presumono accessibili a chiunque vi abbia interesse per la tutela di situazioni giuridicamente rilevanti (artt. 22 e 23 L. 241/1990, modificata dalla L. 11 febbraio 2005, n.15), salvo le eccezioni previste dalla legge (cfr. art. 24, comma1, L. 241/1990 che fa rinvio ad altri segreti come quello sanitario o tributario) e da regolamenti della pubblica amministrazione interessata (art. 24, comma 2, L. 241/1990). Il dovere di rendere accessibili i documenti cessa solo quando viene meno l'obbligo di detenerli (art. 22, comma 6, L. 241/1990). A tali obblighi già esistenti, di recente si sono aggiunti, inoltre, quelli derivanti dal D.Lgs. 33/2013 relativi alla **trasparenza amministrativa** e al nuovo istituto dell'accesso civico, di cui all'art. 5 del decreto citato.

Quanto fin qui riportato sembrerebbe suggerire di ricorrere a modelli di cloud privato che sicuramente presentano meno rischi in relazione sia al trasferimento degli archivi, sia al diritto di accesso ai documenti conservati. La conservazione digitale, però, rappresenta un'attività complessa - sia dal punto di vista tecnologico che organizzativo - che difficilmente amministrazioni piccole e medie riusciranno a gestire "in casa". Proprio per questo motivo, sia il Codice dell'Amministrazione digitale (D.Lgs. 82/2005) che le Regole tecniche (di cui al DPCM 3 dicembre 2013) prevedono la possibilità di acquisire tali servizi da fornitori esterni. Ovviamente resterà sempre in capo alla singola amministrazione l'obbligo di selezionare accuratamente il fornitore e di verificarne l'operato. Già il CAD, infatti, prevede che l'affidamento all'esterno dei servizi di conservazione possa avvenire solo nei confronti di soggetti che offrano idonee garanzie organizzative e tecnologiche (art. 44), ossia di **conservatori accreditati**. Le Regole tecniche, dunque, ribadiscono tale necessità e permettono l'affidamento all'esterno dei servizi di conservazione solo verso conservatori accreditati presso AgID, al contempo prevedendo anche la **possibilità di far certificare il sistema di conservazione da soggetti certificatori** che offrano idonee garanzie organizzative e tecnologiche, ovviamente distinti dai conservatori accreditati.

Il Codice dell'Amministrazione digitale e le nuove Regole tecniche, quindi, per la corretta gestione e la tutela di un archivio elettronico, anche in cloud, prevedono obbligatoriamente la presenza di un team composto dal Responsabile della conservazione (o Digital Preservation Officer), dal Responsabile della sicurezza, dal Responsabile del trattamento dei dati (o Data Privacy Officer) e dal Responsabile del protocollo, che devono operare d'intesa tra loro. Con specifico riferimento alle pubbliche amministrazioni, le figure obbligatorie che devono operare d'intesa fra di loro sono, dunque:

- il Responsabile della conservazione o Digital Preservation Officer (tendenzialmente configurabile nella professionalità di un informatico con conoscenze anche di informatica giuridica, diritto dell'informatica e basi di archivistica), il quale deve coordinare e presidiare i sistemi informatici informativi e documentali garantendone una durata nel tempo;

- il Responsabile per il trattamento dei dati personali o Data Privacy Officer (tendenzialmente riconducibile alla figura professionale di un consulente giuridico/organizzativo che abbia anche cognizioni di informatica e sicurezza informatica oppure di un esperto di sicurezza informatica con cognizioni di diritto), il quale deve occuparsi della protezione del dato nei database e negli archivi digitali;

- il Responsabile del protocollo, dei flussi documentali e degli archivi (un archivista che abbia anche conoscenze base di informatica, informatica giuridica e diritto dell'informatica), il quale deve presidiare la componente archivistica di qualsiasi sistema di conservazione dei documenti informatici.

In tale contesto, dunque, è ormai imprescindibile **valorizzare le figure professionali del Responsabile della conservazione (Digital Preservation Officer) e del Responsabile privacy (Data Privacy Officer)**, titolari di compiti, poteri e funzioni fondamentali per una PA o un'azienda, figure alle quali è necessario garantire, dunque, un'adeguata preparazione, un costante aggiornamento e il riconoscimento delle competenze.

Proprio per dare regolamentazione e il giusto riconoscimento a queste due figure che operano in maniera complementare, è da poco nata l'associazione **ANORC Professioni**, prima associazione italiana che **ha aperto per i Responsabili della conservazione (Digital Preservation Officer) e i Responsabili del trattamento (Data Privacy Officer) due registri nazionali**, istituendo un percorso virtuoso di formazione e aggiornamento a loro dedicato[3].

Infine, rimane da specificare come le modalità di gestione del dato pubblico si intersechino inevitabilmente con i diversi profili di responsabilità dei soggetti che intervengono nella catena di erogazione dei servizi cloud alle PA. Infatti, **l'adozione di tale tecnologia informatica nell'ambito della pubblica amministrazione deve comportare la designazione del cloud provider quale Responsabile del trattamento dei dati (Data Privacy Officer), ai sensi dell'art. 29 del Codice Privacy, con relativa delega in capo allo stesso di una fase importantissima dell'espletamento di un servizio pubblico**. Ed è proprio in virtù di questa delega nella gestione dei dati di rilievo pubblicistico (di cui la stessa PA è Titolare del trattamento) e nell'erogazione di taluni servizi, soprattutto di natura "certificativa", che sembra possibile in alcuni casi configurare una qualifica di incaricato di pubblico servizio per il cloud provider che sia fornitore di una pubblica amministrazione.

[3] http://www.anorc.it/anorc_professioni/

4. WHERE? - Dove sono i dati?

Nell'implementazione di infrastrutture informatiche di cloud è opportuno procedere osservando determinate fasi.

Preliminarmente, occorre individuare **i processi o il flusso di dati che si intendono far migrare nel cloud**, cercando di operare tale scelta in base a un'analisi dei vantaggi e delle criticità e tenendo conto della natura dei servizi che si intende esternalizzare.

In secondo luogo, è necessario procedere a una **classificazione delle informazioni critiche** della struttura, individuando ad esempio le categorie di dati personali, di dati sensibili o di dati ultrasensibili.

Sulla base della tipologia - e della conseguente criticità - dei processi e delle informazioni che si intendono trasferire in cloud, occorre poi individuare il **potenziale ambito geografico di circolazione dei dati e i soggetti coinvolti**, in modo da definire il **quadro normativo di riferimento** per il trattamento e vagliare, in ogni caso, tutti gli aspetti riguardanti **la legge applicabile al rapporto contrattuale** avente ad oggetto la fornitura di servizi cloud.

Con specifico riferimento alla fase di valutazione dei rischi, nella scelta di trasferire i dati di un ente o di un'azienda in cloud occorre comunque considerare **il rischio di indisponibilità, temporanea o definitiva, dei dati in caso di interruzione del servizio**, accidentale o meno.

Dunque, per mitigare l'esposizione dell'azienda ai rischi relativi alla scelta di approvvigionamento in outsourcing di determinati servizi in cloud, **è di estrema importanza adottare una specifica e dettagliata regolamentazione contrattuale** con il cloud service provider, che tuteli le specifiche esigenze individuate dalla pubblica amministrazione o dall'azienda interessata.

Tuttavia, è opportuno considerare che l'utilizzo di sistemi di cloud non implica rischi di natura diversa rispetto a quelli che può presentare la scelta di avvalersi di altri servizi forniti in outsourcing via web, parimenti gestibili tramite la **predisposizione di adeguate clausole del contratto ad oggetto informatico e di dettagliati SLA (Service Level Agreement)**. Al massimo tali rischi vengono "esasperati" da un processo di "esternalizzazione" ampio e diffuso.

Il contratto, dunque, oltre a descrivere e regolare il servizio di cui si intende usufruire e le responsabilità del cloud provider in caso di perdita di dati o di interruzione non accidentale del servizio erogato, soprattutto per i processi più importanti o per i dati sensibili e ultrasensibili dell'azienda, dovrà prevedere nel dettaglio **piani di back up, di disaster recovery e business continuity e dovrà anche contemplare specificamente l'applicazione di norme internazionali o standard ISO di sicurezza informatica**.

Inoltre, dovranno essere previste apposite clausole che disciplinino **la riservatezza delle informazioni e la tutela dei dati personali comuni e sensibili** trattati dall'ente o dall'azienda, l'articolazione delle **responsabilità sull'integrità e la reperibilità** dei dati immagazzinati nella nuvola informatica, **la possibilità di accesso ai sistemi da parte delle autorità, i livelli minimi di servizio garantiti, la durata dei servizi di storage e la portabilità dei dati** (per evitare il c.d. **vendor lock-in**, ossia l'elevata dipendenza da un particolare cloud provider).

Come abbiamo accennato, quindi, grande attenzione deve essere prestata alle modalità di **trattamento dei dati personali comuni e sensibili** nella disponibilità dell'azienda o della PA (alla stregua del D. Lgs. 196/2003). In proposito, il Garante Privacy ha fornito diverse preziose

indicazioni, evidenziando le maggiori criticità presenti nell'utilizzo dei servizi cloud delle quali è necessario tener conto in fase di stesura del contratto.

Sul piano della tutela della sicurezza e della privacy dei dati, soprattutto di quelli della PA, ha molta importanza **l'ubicazione dei dati**, poiché questo costituisce un aspetto estremamente rilevante in base all'attuale disciplina, che prevede il controllo territoriale soprattutto di alcune tipologie di dati, per le quali potrebbe risultare conveniente proseguire il relativo trattamento in house. Inoltre, in fase contrattuale è importante specificare che il cloud provider, in particolar modo qualora fosse fornitore di tali servizi nei confronti della PA, non possa far risiedere i dati pubblici in server allocati in **Paesi extra UE**. Altre specifiche clausole su cui porre la massima attenzione nel contratto con il cloud provider sono quelle attinenti ai **protocolli di interoperabilità del sistema e di portabilità dei dati**, poiché sul punto occorrono specifiche SLA che garantiscano alle pubbliche amministrazioni e alle aziende la possibilità di cambiare il fornitore di servizi cloud senza rischiare di rimanere vittima del fenomeno del **vendor lock-in**.

Soprattutto in riferimento alla protezione dei dati, sarebbe auspicabile l'adozione anche di esplicite clausole di **Privacy Level Agreement ("PLA")** nei contratti con il cloud provider, ossia di una sorta di Service Level Agreement ("SLA") **riferito ai livelli e alle garanzie di tutela e sicurezza dei dati personali** che il cloud provider si impegna a mantenere verso il soggetto contraente.

Questo perché l'adozione di tale tecnologia informatica è inevitabilmente connotata da alcune peculiarità nella regolamentazione giuridica e nella gestione dei rapporti tra i diversi soggetti coinvolti nella fornitura del servizio: il cloud provider, infatti, solitamente assume un ruolo preponderante, rispetto alla PA o all'azienda contraente, circa il profilo della sicurezza, soprattutto riguardo alle scelte sulla **circolazione dei dati nei diversi luoghi (si pensi all'allocazione dei server) e tra distinti soggetti (come, ad esempio, i suoi subfornitori)**.

Quindi, **la legge applicabile e la giurisdizione competente, le c.d. privacy statement (protezione dei dati personali) e la tutela della riservatezza delle informazioni, la disciplina della proprietà intellettuale o i livelli di servizio (SLA), l'accesso ai sistemi da parte delle autorità locali, la ripartizione delle responsabilità nei confronti dei vari soggetti coinvolti, l'interoperabilità e/o la portabilità dei dati in caso di passaggio ad altro fornitore, gli obblighi e le responsabilità in caso di perdita o smarrimento dei dati custoditi dal fornitore, la policy di gestione del salvataggio (backup)** dei dati allocati nella "nuvola" (anche in modalità locale) sono solo alcuni degli aspetti più importanti a cui si deve prestare molta attenzione nella stesura di un contratto che preveda l'affidamento di dati a terzi attraverso l'utilizzo di un sistema cloud.

Una delle maggiori criticità delle tecnologie cloud sta nel fatto che esse consentono di trattare e conservare i dati personali su sistemi di server dislocati in tutto il pianeta, senza avere contezza del luogo fisico in cui sono precisamente ubicati: pertanto, i rischi legati al corretto trattamento sono molto elevati, sia in termini di garanzia della riservatezza e protezione, sia in termini di possibile distruzione, perdita e accessi non autorizzati.

La conservazione dei dati in luoghi geografici differenti, inoltre, ha riflessi immediati sia in relazione alle particolari disposizioni nazionali che disciplinano il trattamento, l'archiviazione e la sicurezza dei dati, sia sulla normativa applicabile in caso di contenzioso tra l'utente di servizi cloud e il cloud provider.

Ovviamente l'outsourcing, e ancora di più la scelta del cloud, estremizza il problema del **"passaggio di consegne" in caso di cessazione degli effetti del contratto**. Infatti, l'utilizzo del servizio di cloud computing da parte delle imprese e delle amministrazioni pubbliche comporta inevitabilmente un trasferimento dei dati dal loro esclusivo controllo, in precedenza esercitato sui sistemi locali, ai sistemi remoti del cloud provider, con tutti i rischi insiti in questa migrazione di dati.

È consigliabile, in ogni caso, cercare di assicurarsi che siano adottate le più ampie garanzie circa la **riservatezza dei dati trasferiti e la persistenza degli stessi anche oltre il tempo previsto per la loro conservazione**, predisporre tutte le misure utili per rendere i dati disponibili in caso di necessità e, soprattutto, privilegiare i servizi che favoriscano **la portabilità degli stessi dati**, ponendo, quindi, particolare attenzione alle clausole contrattuali relative alla cessazione dei servizi. Attraverso tali clausole, l'infrastruttura di un fornitore di servizi informatici (e con particolare riferimento al cloud) dovrebbe garantire che i sistemi sviluppati possano essere sempre trasferiti su piattaforme di fornitori differenti ovvero possano, eventualmente, essere riportati all'interno della struttura informatica del cliente con il minimo impatto, così da evitare il rischio di doversi legare a un unico provider (fenomeno definito **vendor lock-in**).

Per proteggere la confidenzialità dei dati, occorre valutare anche **le misure di sicurezza** utilizzate per consentire l'allocazione dei dati in cloud, privilegiando i fornitori che utilizzano tecniche di **trasmissione sicure, tramite connessioni cifrate coadiuvate da sistemi di identificazione dei soggetti autorizzati all'accesso**: ovviamente, la complessità di tali misure di sicurezza deve essere commisurata alla criticità dei dati

Nell'ipotesi in cui il trattamento riguardi particolari tipologie di dati, infatti, come i dati strategici, personali o addirittura sensibili, per i quali sono maggiormente pressanti le esigenze di riservatezza, si raccomanda **l'utilizzo di protocolli sicuri nella fase di trasmissione e la conservazione in forma cifrata sui sistemi del fornitore di servizio**.

In generale, proprio in considerazione del fatto che nella prassi contrattuale tali prerogative permangono comunque in capo al cloud provider, occorre considerare che, sebbene sia indiscusso che l'azienda o la PA che acquisti servizi cloud debba essere senz'altro considerata quale "**Titolare di trattamento**", ci sono alcuni problemi di inquadramento giuridico per il fornitore di servizi di cloud computing.

Il provider, infatti, qualora residuino spazi di autonomia decisionale riguardo alle modalità di trattamento dei dati personali degli interessati, potrebbe essere considerato, insieme all'azienda o alla PA, quale Titolare autonomo del trattamento ex art. 28 d.lgs. 196/2003 (Codice Privacy).

Ai sensi della vigente normativa privacy, in effetti, sembrerebbe più ragionevole la scelta di una soluzione basata sulla titolarità autonoma tra i due soggetti coinvolti.

Diversamente, ove il titolare riesca a impartire istruzioni specifiche e dettagliate al cloud provider in ordine alle finalità e alle modalità di trattamento dei dati, nonché a esercitare quel controllo tipico del rapporto titolare-responsabile, il fornitore di servizi cloud dovrà essere nominato Responsabile ex art. 29 del Codice Privacy.

Ricordiamo che in caso di trattamento dei dati pubblici sia il ruolo di Titolare, sia quello di Responsabile (Data Privacy Officer), comporta una delega in capo allo stesso cloud provider di una fase importantissima dell'espletamento di pubblici servizi.

5. WHEN? - La fase delle trattative precontrattuali

In genere, le principali difficoltà di comprensione del contratto ad oggetto informatico dipendono da:

- **la disparità culturale informatica tra fornitori di servizi informatici e clienti (tenendo presenti, tuttavia, gli obblighi di informazione dei fornitori verso i clienti, in ossequio ai canoni di correttezza e buona fede nelle trattative precontrattuali, ai sensi dell'art. 1337 del Cod. Civ.);**
- **"atipicità standardizzata" dei contratti ad oggetto informatico (contratti misti e di difficile inquadramento sistematico);**
- **l'internazionalità dei servizi informatici e telematici di cui ai contratti ad oggetto informatico.**

Relativamente ai contratti cloud, occorre inoltre considerare ulteriori criticità:

- **internazionalità implicita**

Quale legge si applica al rapporto contrattuale intercorrente tra provider e cliente?

Ci sono delle clausole contrattuali redatte con formule standard che possono essere nulle per un determinato ordinamento (fenomeno della c.d. atipicità standardizzata)?

Quale Autorità Giudiziaria è competente a decidere sull'interpretazione di quel contratto?

In quale Stato si aziona il diritto?

- **ubicazione dei dati**

Conosciamo il luogo dove è allocato lo spazio di memoria?

Queste località godono di un adeguato servizio di sorveglianza territoriale?

- **privacy**

Abbiamo la garanzia che la cifratura sia disponibile a tutti i livelli e che tale crittografia sia fornita da esperti del ramo?

Si possono impiegare i sistemi cloud per controllare le attività dei clienti (e dei dipendenti)?

- **responsabilità in caso di accessi abusivi e dispersione dei dati**

Chi è il soggetto responsabile in caso di perdita dei dati?

Cosa accade ai dati qualora il cloud provider interrompa la fornitura del servizio?

Proprio alla luce della presenza di tali fattori di incertezza, occorre dunque valutare il rapporto tra rischi e benefici per l'azienda o la pubblica amministrazione, riducendo i primi sia mediante un'attenta e oculata scelta del modello di cloud che si intende implementare, sia attraverso la **predisposizione di una regolamentazione contrattuale completa anche di norme in tema di responsabilità e dedicata alle specifiche esigenze del cliente di servizi cloud**.

I contenuti dei contratti aventi a oggetto i servizi cloud, in ogni caso, possono essere molto diversi in base al modello di erogazione e alla tipologia stessa di servizi di cui si intende usufruire: pertanto è opportuno porre particolare attenzione alla presenza di clausole troppo

generiche o di scarsa trasparenza, o che addirittura contemplino l'esonero da responsabilità del cloud provider.

5.1 Ma gli enti e le aziende come possono orientarsi fra le innumerevoli offerte disponibili sul mercato?

Come dicevamo, in sede di redazione del contratto dovranno evitarsi le clausole standard, cercando invece di prediligere la predisposizione di clausole appositamente redatte per il singolo rapporto contrattuale (e non già imposte unilateralmente dal cloud provider come purtroppo spesso succede).

Inoltre, un buon contratto di outsourcing di servizi di conservazione dei documenti in cloud non dovrà limitarsi alla corretta applicazione delle norme contenute nel Codice Civile e nel Codice Privacy (regolamentando i processi di sicurezza e privacy e stabilendo con quali modalità e da chi viene garantita la sicurezza informatica dei dati), ma dovrà prevedere anche **l'applicazione di norme internazionali o standard ISO** (come ad esempio la ISO 27001, la ETSI TR 101 533, UNI 11386- SinCRO, etc.).

Le responsabilità derivanti dall'utilizzo di tecnologie cloud computing nella fornitura di servizi di conservazione digitale, pertanto, devono essere previste da un'analisi a monte che rifletta nel relativo contratto i termini delle responsabilità in capo sia al fornitore del servizio sia ad eventuali intermediari (che concorrano all'erogazione del servizio finale) o al Responsabile della conservazione (ossia il Digital Preservation Officer, inteso quale persona giuridica a cui delegare parte dei processi, compresi quelli relativi all'archiviazione delle informazione nella "nuvola informatica").

Di conseguenza, nel gestire al meglio la contrattualizzazione del servizio di cloud computing applicato ai processi di conservazione digitale risulta fondamentale l'applicazione di quel concetto di **"interoperabilità intellettuale" tra legali, informatici, archivisti** e coloro che, in qualità di **responsabili** (interni o esterni all'organizzazione), gestiscono il processo di conservazione digitale dei documenti.

5.2 E nelle PA?

Con specifico riferimento alle pubbliche amministrazioni, abbiamo già espresso come i servizi cloud costituiscono uno dei mezzi più economici per raggiungere l'effettiva realizzazione di quel sistema di **eGovernment** delineato dal **Codice dell'Amministrazione Digitale**, le cui norme sono finalizzate anche al conseguimento degli obiettivi di efficacia, efficienza, trasparenza, partecipazione, condivisione, cooperazione, interoperabilità e sicurezza dell'agire amministrativo.

Le valutazioni inerenti alle modalità di implementazione delle infrastrutture cloud nelle pubbliche amministrazioni italiane appaiono ormai non più differibili, dal momento che il nostro legislatore ha ormai previsto la possibilità di avvalersi di tali sistemi.

A tal riguardo occorre considerare quanto disposto dall'Agenda digitale italiana: con l'art. 47 della legge n. 35/2012 (di conversione del D.L. n. 5/2012) è stato introdotto il comma in cui si dettaglia il programma di misure da adottare, appunto, per il perseguimento degli obiettivi **dell'Agenda digitale italiana**, tra le quali, alla lett. d) dell'art. 47, è espressamente menzionata la *"promozione della diffusione e del controllo di architetture di cloud computing per le attività e i servizi delle pubbliche amministrazioni"*.

Negli aspetti da valutare nell'adozione di un sistema cloud per una PA il tema di maggior rilievo è sicuramente quello relativo alle modalità di gestione dei dati pubblici, che si interseca inevitabilmente con quello dei diversi profili di responsabilità che possono configurarsi sia in capo ad alcuni organi della PA, sia in capo ai diversi soggetti che intervengono nella catena di erogazione dei servizi cloud alla PA.

In ogni caso, è opportuno che la PA proceda preliminarmente ad effettuare **un'analisi comparativa (prevista anche all'art. 68 del Codice dell'Amministrazione Digitale**) in merito ai possibili modelli di cloud implementabili e che la scelta del cloud provider sia effettuata tenendo conto di sistemi di qualificazione del concorrente basati su elevati standard qualitativi, alla stregua dei quali l'aggiudicatario dovrà essere individuato secondo il criterio dell'offerta economicamente più vantaggiosa.

Nello specifico, sono possibili **soluzioni di digital preservation in cloud** che utilizzino differenti modelli di fruizione. Proprio per la PA le soluzioni di community cloud, ad esempio, rappresentano un'ottima alternativa al private cloud, consentendo a varie amministrazioni di fare sistema. Ad ogni modo anche il cloud pubblico è utilizzabile, soprattutto nei casi in cui la sua adozione sia accompagnata da un'attenta valutazione interna all'amministrazione e da una successiva contrattualizzazione degli aspetti maggiormente delicati.

A prescindere dal modello prescelto, infatti, soprattutto per i servizi di conservazione occorrerà, come già accennato, prestare la massima attenzione alla scelta del **conservatore esterno** mediante la realizzazione di idonei capitolati e contratti.

Il contratto, infatti, assume un ruolo fondamentale nella regolamentazione dei rapporti tra committente e fornitore di servizi in cloud: questo, oltre a descrivere e regolare il servizio di cui si intende usufruire e le responsabilità delle parti, nel caso di conservazione digitale dei documenti dovrà tener presente anche l'eventuale richiamo e l'applicazione di norme internazionali o standard ISO di sicurezza informatica; inoltre, in considerazione del fatto che i dati da gestire non risiedono presso la propria struttura ma sono distribuiti su siti geograficamente distinti (in modo tale da non permettere al titolare di quel dato di conoscere il luogo effettivo di conservazione degli stessi), si pongono alcune problematiche legate all'applicazione di stringenti misure di sicurezza e di clausole di riservatezza *ad hoc*.

Attualmente **non esistono delle norme specifiche, nazionali o comunitarie, che disciplinino l'erogazione di servizi di cloud computing**, sebbene la qualificazione giuridica di un contratto di servizi cloud risulti essenziale al fine di determinare quale sia la disciplina giuridica da applicarsi ai rapporti tra le parti contrattuali (PA e cloud provider) e, di conseguenza, quali clausole sia opportuno inserire nel contratto.

Tuttavia, è utile rilevare che i modelli contrattuali solitamente proposti dai cloud provider appartengono prevalentemente alla categoria dei **contratti c.d. "per adesione"** nei quali, sostanzialmente, le clausole non sono negoziabili e spesso non sono esaustivamente disciplinati profili giuridici assai delicati (come le responsabilità, i livelli di servizio, le modalità di recesso o la legge applicabile) rischiando, quindi, di non garantire la necessaria tutela alle aziende o alle PA contraenti.

Inoltre, occorre **prestare attenzione ai documenti scambiati nella fase precontrattuale** (lettere di intenti, *memorandum of understanding*, attività di *due diligence*, verbali di assemblee etc.), perché possono avere un valore nell'interpretazione successiva di clausole contrattuali o addirittura integrare clausole mancanti e/o generare responsabilità.

Di conseguenza, **le premesse del contratto** devono sempre sintetizzare le trattative intercorse, sottolineare lo scopo del contratto (e, quindi, la reale volontà delle parti - come i doveri reciproci di informativa) e soprattutto annullare i documenti pregressi.

Alla luce delle considerazioni effettuate, dunque, il problema relativo alla gestione dei dati in *cloud* richiede un'approfondita analisi non tanto in termini di natura tecnico-informatica, aspetti sotto i quali il cloud presenta considerevoli vantaggi, quanto piuttosto sotto il **profilo negoziale e contrattuale**, strettamente correlato anche alla possibilità per l'azienda o la PA di contrattare effettivamente con il cloud provider l'inserimento di determinate clausole.

È auspicabile, dunque, procedere nella scelta del modello di cloud adottando **il metodo del *Cloud design service***, che consente di progettare l'implementazione e la fruizione dei servizi cloud in modo adeguato ai differenti gradi di criticità che possono di volta in volta connotare il trattamento delle diverse tipologie di dati di una struttura aziendale o di una pubblica amministrazione.

Una contrattualizzazione mirata e improntata al criterio del *cloud design*, infatti, permetterebbe una graduale introduzione delle tecnologie cloud nella struttura dell'azienda o della PA e implicherebbe un minore impatto dal punto di vista organizzativo e di formazione del personale, consentendo anche alla platea di stakeholder e utenti interessati di godere dei maggiori livelli di efficienza conseguiti.

6. Conclusioni - Quali sono, dunque, le regole da seguire?

SIGNORI, BENVENUTI AL FIGHT CLOUD

Prima regola del Fight Cloud:
NON SOTTOVALUTATE MAI IL FIGHT CLOUD .
Seconda regola del Fight Cloud:
NON DOVETE SOTTOVALUTARE MAI IL FIGHT CLOUD .
Terza regola del Fight Cloud:
SE QUALCUNO GRIDA BASTA, VUOLE LA PORTABILITÀ, SERVE UNA CLAUSOLA.
Quarta regola:
SI MEMORIZZANO SOLO DATI CIFRATI.
Quinta regola:
TENETEVI LE VOSTRE CHIAVI D'ACCESSO, RAGAZZI.
Sesta regola:
NIENTE DATI SUL CLIENT, NIENTE BACKUP.
Settima regola:
L'IMMAGAZZINAMENTO VIRTUALE DURA PER TUTTO IL TEMPO NECESSARIO.
Ottava e ultima regola:
SE QUESTA È LA VOSTRA PRIMA VOLTA AL FIGHT CLOUD... DOVETE COMBATTERE!

Il cloud computing, in effetti, ha le sue regole. Non ne si può prescindere, i rischi per la privacy e per la sicurezza di dati e informazioni sono incalcolabili. Ma le opportunità sono altrettanto sconfinate ed estremamente affascinanti.
Tuttavia, si commetterebbe una grave ingenuità se si sottovalutassero le fondamentali implicazioni sotto il profilo della sicurezza delle informazioni che vengono immagazzinate virtualmente, specialmente per quanto riguarda i dati di rilevanza pubblicistica, i dati strategici

e i dati personali sensibili. È, perciò, necessaria l'adozione di sistemi e applicazioni informatiche che permettano un sempre maggiore sfruttamento delle enormi potenzialità e dei vantaggi del cloud e, al tempo stesso, garantiscano la possibilità di mantenere il controllo delle informazioni memorizzate.
Queste istanze di tutela possono essere perseguite attraverso diverse soluzioni tecniche, come quelle già offerte dall'hybrid cloud, non inteso in riferimento al segmento di mercato (che individua l'area di servizi cloud predisposti per la condivisione tra più utenti e al contempo dedicati a singoli soggetti o gruppi), bensì come architettura ICT che affianca e integra servizi di cloud computing implementati sia internamente, sia esternamente alla singola organizzazione. Ciò consente di utilizzare il cloud interno alla stessa struttura organizzativa per la memorizzazione delle informazioni più sensibili o strategiche e il cloud esterno per l'immagazzinamento e la condivisione di dati meno confidenziali.
Imprescindibile, invece, è l'utilizzo di sistemi di cifratura dei dati memorizzati in cloud e, soprattutto, la diligente custodia delle chiavi d'accesso da parte del Responsabile (Data Privacy Officer).
Eppure non basta.
Da una differente prospettiva, il controllo dei dati che vengono inviati "fra le nuvole" non può essere assicurato senza una puntuale e lungimirante contrattualizzazione della fornitura dei servizi, ovviamente ritagliata sulle specifiche esigenze del customer cloud.
Devono essere previste, in ogni caso, apposite clausole che disciplinino la riservatezza delle informazioni, la proprietà intellettuale delle opere, l'articolazione delle responsabilità sull'integrità e la reperibilità dei dati immagazzinati nella nuvola informatica, la possibilità di accesso ai sistemi da parte delle autorità, i livelli minimi di servizio garantiti, la durata dei servizi di memorizzazione e la portabilità dei dati (per evitare il c.d. vendor lock-in, ossia l'elevata dipendenza da un particolare cloud provider).
Ma tutto ciò non deve spaventare. Basti pensare che sono già in via d'implementazione soluzioni di cloud governance progettate per le strutture di quella organizzazione che, nell'immaginario di tutti, costituisce senza dubbio l'iconica rappresentazione del paradigma della sicurezza delle informazioni: ebbene sì, cloud computing anche per il sistema delle agenzie governative federali U.S.A.!
Del resto... qualcuno ha detto che si deve avere coscienza, non paura.

7. Schema e principali allegati di un contratto di Servizi di cloud computing

- Premesse e Definizioni
- Oggetto e Finalità
- Specificazioni Tecniche del servizio affidate a uno o più allegati
- Modalità di perfezionamento del contratto
- Livelli e Modalità di mantenimento del servizio e assistenza
- Corrispettivi (pay for use o canoni per servizi differenziati)
- Responsabilità fornitore e Responsabilità Cliente (eventuale possibilità di sospensione del servizio)
- Recesso e risoluzione (con clausola risolutiva espressa)
- Obblighi di riservatezza (anche successivi alla conclusione del contratto)
- Proprietà e licenze delle prestazioni oggetto del contratto (software anche di terzi, domain name, loghi etc.)
- Fase patologica (controversie, fallimento del Fornitore del servizio e del Cliente etc.)
- Passaggio di consegne (fruibilità del DB/Archivio/Soluzione dopo cessazione effetti del contratto)
- Modalità delle comunicazioni e protezione dei dati
- Modifiche del contratto e Cessione del contratto
- Durata del contratto
- Legge applicabile e Giudice Competente (o Arbitro)

Allegati

- SLA [livelli di servizio su accessibilità alla piattaforma, livelli di servizio su modalità di ripristino, livelli di servizio su tempistiche di assistenza (e risoluzione) in caso di problemi di utilizzo, livelli di utilizzabilità della piattaforma e verifica di eventuali rallentamenti nella fornitura del servizio, livelli di servizio sul mantenimento dei dati (e documenti) etc.] e penali (ed eventuali delimitazioni dell'indennizzo – ammissibilità anche in caso di colpa grave o violazione di misure di sicurezza minime, necessarie o idonee);

- Policy di utilizzo della piattaforma;

- Privacy Policy con nomina in capo al cloud provider come Responsabile del trattamento - Data Privacy Officer (e Amministratore di Sistema), definizione di misure di sicurezza a presidio della piattaforma (definizione di politiche di prevenzione da accessi abusivi con definizione di tecniche funzionali al controllo degli accessi e di verifica dell'integrità dei dati e di monitoraggio/reporting in caso di accessi abusivi con eventuale perdita parziale del dato);

- Specificazioni Tecniche su soluzioni fornite e tecnologia utilizzata;

- Eventuali Certificazioni ottenute.