Università degli Studi di Salerno

Dipartimento di Diritti della Persona e Comparazione – DIRPE

DOTTORATO DI RICERCA
"COMPARAZIONE E DIRITTI DELLA PERSONA"
Coordinatore Ch.mo Prof. Pasquale Stanzione

XIII CICLO

TESI DI DOTTORATO

" CLOUD COMPUTING;RISVOLTI NORMATIVI "

Il coordinatore:
Ch.mo Prof. Pasquale Stanzione

Tutor della dottoranda: **Dottoranda:**
Prof. Antonio Musio **Marilena Limone**

Anno Accademico 2013/2014

Ai miei Genitori, la mia più grande forza.
E a Te.

Introduzione

Sul finire degli anni ’70 del secolo scorso una nuova, rivoluzionaria, scoperta si affaccia al mondo per poi progressivamente affermarsi: l’informatica[1].

Dopo l’orrore e la devastazione delle guerre e dopo che grossa parte dell’ingegno umano più arguto si era impegnato nella creazione del male e nella costruzione dei modi più atroci per praticarlo, ecco il risveglio delle coscienze e delle intelligenze porsi, finalmente, al servizio del bene e avvertire l’immanente esigenza di muoversi nel senso della ricostruzione. Ricostruzione valoriale innanzitutto - la Dichiarazione Universale dei Diritti dell’Uomo - , ricostruzione spirituale e allontanamento dall’abominio passato - il processo di Norimberga - , ricostruzione materiale e strumentale di beni e di cose da porre al servizio della nuova umanità *in aedificando*.

[1] Il termine *informatica* deriva dalla crasi dell’espressione francese *information automatique* ed indica la gestione automatica di dati e di informazioni mediante calcolatore. Coniato nel 1962 da Philippe Dreyfus - docente dell’Università di Harvard, che nel 1950 utilizzò Mark I, il primo computer automatico - ha avuto una notevole diffusione in Italia nella seconda metà degli anni Sessanta. Oggi, il termine *informatica* ha assunto altresì il significato di disciplina scientifica e sta *per scienza dell’uso dell’elaboratore elettronico (computer science).*

Tra questi, arriva la rivoluzione tecnologica, e in essa e anzi prima di essa, che ne è l'anima, l'informatica.

Dal primo calcolatore elettronico, brevettato tra il 1936 e il 1938 dall'ingegnere tedesco Konrad Zuse ai *garages* americani trasformati in celebri laboratori da Bill Gates e Steve Jobs, l'informatica ha conosciuto uno sviluppo rapidissimo e inarrestabile ed una diffusione tale da risultare oggi uno strumento operativo indispensabile per le relazioni interpersonali ed i processi economici[2]; il concetto stesso di "società globale" è, per la quasi totalità, figlio dell'informatica e del travolgente impatto che essa ha avuto in termini di abbattimento delle limitazioni spazio-temporali in ordine alla circolazione ed allo scambio della più svariata pluralità di informazioni, beni e servizi.

Il diritto, dal canto suo, col passar del tempo si è visto obbligato a recepire il mutamento economico e socio-culturale collegato a questa grande

[2] Ciò grazie, soprattutto, alla telematica. Il termine telematica deriva dall'avverbio greco "tele", che significa lontano, e dal suffisso "ema" che indica quell'elemento funzionale che dà forma a qualcosa. Thélème era anche l'abbazia immaginaria con cui Gargantua, il mitico gigante nato dalla penna di François Rebelais – scrittore francese umanista del XVI secolo – prefigurava un mondo di completa libertà. A differenza di tutte le altre, era un'abbazia senza muraglie e barriere esterne: tutti vi potevano entrare, bene accolti, qualcuno si poteva smarrire. Oggi, per telematica si intende un insieme di servizi informatici, dunque, basati sul codice binario, offerti e fruiti, in tempo reale, attreverso una rete di telecomunicazione.

innovazione e ha tentato, di volta in volta - ma non sempre con grande successo - di positivizzarlo, dettandone regole e limiti fino, a creare al interno un vero e proprio settore dedicato all'informatica, il diritto dell'informatica appunto, che prende in esame i problemi giuridici all'utilizzo della stessa nei rapporti interpersonali, unitamente alla telematica.

Col tempo, l'evoluzione ha portato all'acquisizione di una autonomia sia formale che sostanziale del diritto dell'informatica, il quale ha, così, cessato di essere una mera branca dell'informatica giuridica per assurgere a vera e propria *scientia juris;* ciò perché la diffusione delle tecnologie informatiche ha imposto ai legislatori di tutto il mondo[3] di creare da un lato norme *ad hoc*, capaci di disciplinare i nuovi fenomeni sociali, come ad esempio quello della tutela delle

[3] A testimonianza di questa esigenza, il 30 aprile del 1980, il Consiglio d'Europa, con l'approvazione della Raccomandazione *"Informatica e diritto"*, promuoveva già allora l'insegnamento, la ricerca e la diffusione in materia d'informatica e diritto. La Raccomandazione prevedeva, in particolare, di considerare l'elaboratore elettronico come fondamentale strumento di lavoro, anche e particolarmente per il giurista, invitandolo per tanto ad approfondire, accanto alle problematiche specifiche dell'informatica, anche le applicazioni e gli strumenti giuridici legati alla protezione dei dati immessi negli elaboratori stessi ed alla sicurezza informatica.

banche dati, dall'altro, di reinterpretare i precedenti normativi al fine di adattarli alle nuove realtà, a cominciare dalla disciplina dei contratti[4].

Oggi il mondo dell'informatica, sempre in continua espansione, affronta una nuova, grande, sfida con l'introduzione di una tecnologia ancora una volta rivoluzionaria, la quale, azzerando una volta per tutte le distanze, annulla il problema della segregazione delle informazioni in singoli dispositivi o apparati e consente una circolazione, un accesso ma soprattutto una archiviazione quasi totalmente illimitati e senza restrizioni; questa nuova tecnologia si chiama c*loud computing.*

Con questa espressione ci si riferisce ad una modalità di fruizione dei servizi informatici non soltanto nuova ma anche alternativa, che non si realizza più attraverso il necessario, preventivo, acquisto del *software,* ma prende corpo attraverso il più semplice utilizzo della risorsa, svincolato dal concetto di proprietà, per mezzo della sua erogazione. Ma vi è di più; il *cloud* è anche la possibilità di conservare e di elaborare grandi quantità di informazioni via internet.

[4] Sull'argomento M.G.. LOSANO , *Informatica Giuridica*, in *Dig. Civ., IX,* Torino, 1993, pp. 417-420

La *"nuvola"* - questa è la traduzione italiana di *cloud* – consente, pertanto, di usufruire di una notevole pluralità di servizi, anche assai complessi, senza doversi necessariamente dotare nè di *computer*, nè di *hardware* avanzati, né di personale in grado di programmare o gestire i sistemi correlati.

La tecnologia del *cloud computing*, che garantisce, oggi, soluzioni innovative per gestire molteplici attività con efficienza e possibilità di grande risparmio, presenta tuttavia, quale risvolto della medaglia, criticità e rischi, soprattutto per la *privacy*, di cui sarà bene tenere conto.

Questo lavoro si pone come obiettivo quello di analizzare i risvolti normativi collegati al sempre più massiccio utilizzo della tecnologia del *cloud computing* nei più svariati settori della vita quotidiana, dall'uso domestico a quello aziendale, per finire alla Pubblica Amministrazione e di valutarne il complesso stato dell'arte, ovvero l'adeguamento delle prescrizioni normative in materia di trattamento dei dati personali, ma anche in ordine ai rapporti contrattuali sottesi, ai nuovi strumenti di accesso e trattamento delle informazioni, allo scopo, tra l'altro,

d’individuare le modalità mediante le quali sia possibile armonizzare la disciplina interna con il quadro normativo comunitario.

CAPITOLO PRIMO

IL CLOUD COMPUTING

Sommario: *1. Definizione e utilizzo - 2. I servizi offerti – 3. Profili tecnici: la divisione tra Pubblic e Private Cloud -*

1. Definizione e utilizzo

Comprendere a fondo la portata di una rivoluzione, in qualunque sfera essa occorra, proprio mentre essa è in pieno svolgimento, è impresa ardua, se non impossibile. Come prevedere quali e quante tra le promesse o le minacce, le aspettative o i timori saranno confermati dopo dieci o venti anni? E quante volte ciò che sembrava una rivoluzione al momento, riconsiderata con la consapevolezza che la storia ci regala, si rivela poi una semplice correzione di rotta o una superficiale agitazione? E tuttavia in nessun momento previsioni, attese, speranze, certezze si manifestano come nel corso di una rivoluzione.

È questa la situazione in cui ci troviamo oggi: la rivoluzione digitale promette, attraverso i suoi sostenitori e i suoi protagonisti, di cambiare radicalmente e in meglio sia il funzionamento globale della società sia la vita degli individui. E naturalmente, tale situazione genera simmetriche paure tra quanti temono, invece, che tali cambiamenti si possano rivelare involuzioni e regressioni. Le tensioni ideologiche sono, poi, tanto più acute in quanto alla base del cambiamento si pone una pervasiva diffusione della tecnologia nella vita quotidiana e sociale. D'altra parte, facilmente si può riscontrare come e quanto sia oggetto di dibattito lo stesso ruolo determinante dell'innovazione tecnologica nel più generale mutamento sociale in corso.

Negli ultimi tempi si parla molto e in molti settori di *cloud computing*; questa è una delle tecnologie di maggiore successo degli ultimi anni e, secondo le previsioni degli esperti, nel prossimo futuro promette di rivoluzionare il mondo dell'*information technology* che noi conosciamo, ancor più di quanto non lo abbia già fatto.

Col termine *cloud* - o *nuvola* - si suole indicare, in modo metaforico quasi a sottolinearne l'immaterialità, il mondo di internet. La nube, infatti, è il simbolo più frequentemente utilizzato per descrivere la Rete non solo, nei diagrammi tecnici, quanto anche praticamente, utilizzandola come icona sui i tasti dei pc e dei *tablet*.

Col passare del tempo, questo simbolo è stata progressivamente impiegata per indicare - anche e soprattutto - la nuova gamma di risorse e servizi IT[5] disponibili in internet; oggi, con l'espressione *cloud computing* si suole definire l'insieme di risorse e tecnologie informatiche alle quali sia possibile accedere direttamente *on-line*, rese disponibili da fornitori - speciali e un po' particolari, si analizzerà in seguito in che senso - sotto forma di erogazione di un servizio.

Il *cloud computing* si è affermato proprio grazie al sempre maggiore uso di internet ed alla diffusione capillare dei dispositivi mobili come una strategica opportunità di agevole, economico e costante accesso alle risorse offerte dall'informatica inizialmente per i soli privati con un uso precipuamente dilettevole, successivamente per

[5] Infrastrutture, piattaforme e software.

le aziende, i professionisti e addirittura, in epoche recentissime, anche per le Pubbliche Amministrazioni con conseguenze estremamente significative che si proverà ad analizzare innanzi.

Paradossalmente, se lo strumento principe correlato ad internet è sempre stato, fino ad epoche piuttosto recenti, il *personal computer*, i nuovi processi di innovazione tecnologica hanno posto in minoranza l'importanza di questo oggetto; il sintomo più importante di questo cambiamento è proprio dato dalla crescita esponenziale dell'utilizzo dei servizi di *cloud computing* e della consequenziale possibilità di eseguire applicazioni e archiviare dati direttamente sul Web[6] piuttosto che sui propri pc, mai abbastanza capienti e ormai diventati oggetti ingombranti.

Ed è importante sottolineare che parrebbe proprio non trattarsi della moda del momento; questo perché i vantaggi scaturenti dall'utilizzo della *nuvola* sono riscontrabili innanzitutto sul piano economico - quello che conta evidentemente di più - prima ancora che pratico; il *cloud*, infatti, nasce per ridurre i costi e migliorare la produttività, tanto quella

[6] Ovvero sui computer, molto più "capienti", dei provider dei servizi di cloud.

professionale quanto quella lavorativa e - perché escluderlo - per migliorare la qualità della vita degli utenti.

Come vedremo, la possibilità di poter accedere a dati, documenti e programmi da qualunque posto nel mondo rappresenta una (ri)evoluzione di portata epocale e molto affascinante, perché, ancora una volta, porta ad un accorciamento - sarebbe meglio forse dire un quasi azzeramento - delle distanze.

Tutto ciò considerato, un miglioramento della qualità della vita, seppur sotto un aspetto abbastanza settoriale e dedicato ad una ristretta utenza - che tuttavia è in netta espansione - è innegabile; più tecnicamente, proviamo a spiegare come esso avviene.

.2 Servizi e vantaggi

Cosa s'intende esattamente per *cloud computing*?

Secondo la definizione dell'*ACM Computer Communication Review*

" I sistemi di *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"[7] .

Volendo provare a tradurre questa definizione, ad una prima lettura forse un po' troppo complessa, il *cloud computing* è un sistema di implementazione di risorse basato su "nuvole" di *computer*, realizzati e gestiti da grossi *providers*, in grado di fornire ai *clients* finali servizi di *storage* e *processoring.*

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

Come già accennato, tale sistema rappresenta, per le sue caratteristiche, la soluzione del momento per molte aziende e professionisti, grandi e piccoli, che hanno bisogno ciclicamente di notevoli risorse e che non sono in grado di sostenerne gli ingenti costi.

Come già detto infatti, da qualche anno questa espressione ha iniziato ad essere utilizzata per definire il servizio di messa a disposizione dell'utente, da parte di fornitori qualificati, di un insieme di tecnologie e di risorse informatiche, accessibili direttamente *on-line*[8], senza più la necessità di archiviare il servizio nella memoria del proprio pc e senza lo scomodo effetto di segregazione che da ciò discendeva, ma soprattutto a un costo assai più basso di quello che sarebbe stato necessario sostenere per acquistare direttamente quel determinato programma.

[8] Per una definizione di dettaglio, cfr: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *The NIST Definition of Cloud Computing. Recommendations of the national Institute of Standards and Technology,* September 2011, p. 2 ss., all'indirizzo http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; P. MELL - T.GRACE, *The NIST Definition of Cloud Computing*, version 15, 7 ottobre 2009, in http://csrc.nist.gov/groups/SNS/cloud-computing/. Ancora, nel dettaglio, in relazione al cloud computing: IBM, *Diradare le nebbie attorno al cloud computing*, Segrate, 2010; NEXTVALUE, *Cloud computing un anno dopo. CIO italiani e CIO europei a confronto,* Milano, 2010, 28, fig. 12 e 13, 30 e ss.

Tecnicamente perciò, tale servizio rende possibile al suo fruitore l'utilizzazione di spazi di memorizzazione, di *software*, di *server* virtuali e di virtuali e di qualsivoglia altra tipologia di ambiente di sviluppo, senza più più che le risorse relative risiedano nei sistemi informatici dello stesso, bensì bensì mediante il collegamento a *server* remoti, gestiti da terze parti, i c.d. c.d. *cloud provider*[9].

In altre parole, sfruttando la tecnologia del *cloud computing,* gli utenti collegati al fornitore del servizio possono compiere tutte le attività elencate e migliaia di altre ancora, con significativi vantaggi: primo tra tutti, quello di poter accedere ai propri dati da qualsivoglia pc, *tablet* o *smartphone* ovvero quello di avere a disposizione memorie di massa praticamente senza limite perciò non necessitando più di capienti dischi all'interno dei singoli apparecchi o di supporti esterni mobili da collegare. Un'unica necessità : la connessione ad internet.

---

[9] Per un'analisi tecnico-informatica dei sistemi di *cloud computing*, delle loro architetture e del loro funzionamento, cfr. SUN MICROSYSTEMS, *Introduction to Cloud Computing Architecture. White Paper, 1st Edition, giugno 2009, in http://webobjects.cdw.com/webobjects/ media/pdf/Sun_CloudComputing.pdf.* Per uno studio che tiene conto anche delle dinamiche economiche, si veda inoltre AA.VV., *Above the Clouds: A Berkeley View of Cloud Computing,* 10 febbraio 2009, in http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html. Cfr. inoltre EXPERT GROUP REPORT, *The Future Of Cloud Computing, rapporto redatto per la Commissione europea, 2010,* in http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

I sistemi di *cloud computing* si caratterizzano principalmente per la loro "scalabilità" ovvero per la flessibilità nell'erogare quantitativamente le risorse informatiche in ragione delle esigenze concrete individuali, diversamente da quanto accade per le risorse aziendali, che devono essere stimate sui livelli massimi di utilizzo per poter consentire di fare fronte a tutte le potenziali necessità, sebbene ciò possa comportare un loro diffuso sotto-utilizzo[10].

L'importanza strategica del *cloud computing* risiede nel fatto che la sua diffusione su larga scala consentirebbe il superamento definitivo dell'assetto che si è avuto sino a ieri, caratterizzato da una miriade di *clients* remoti, dotati di una propria autonoma postazione o di propri *server " in house"*[11] in favore di un regime di *" Software as a Service"*[12], consistente nel servirsi di *software* e *hard disk* messi a disposizione dai gestori delle nuvole e accessibili tramite *browser web*.

[10] L'ottimizzazione delle risorse informatiche può, dunque, avvenire anche attraverso un'integrazione fra quelle aziendali, destinate a sostenere i flussi lavorativi ordinari, con quelle di cloud computing, volte a soddisfare quelle eccezionali. Secondo alcuni operatori, poi, il cloud computing potrebbe rivelarsi una soluzione facilitante i processi di fusione/acquisizione fra imprese, semplificando e riducendo i costi di integrazione fra le risorse informatiche.

[11] Si pensi alle aziende ed alla mole di dati che si trovano a gestire.

[12] O anche *"Storage as a Service"*.

Non più programmi da far girare né dati da archiviare su singoli pc quindi, ma grossi sistemi integrati, indefiniti, di *server* e processori, dai quali attingere capacità di memoria e di processo a seconda delle singole concrete esigenze.

Tale sistema si costruisce attraverso l'esternalizzazione dei servizi IT dai *clients* finali ai *provider* di nuvole. In tal modo, perciò, le aziende o i professionisti smettono di gestire al proprio interno dati e applicazioni, delegando tali operazioni in *outsourcing*, con un grosso risparmio sulla gestione del personale e delle strutture fisiche IT.

Riguardo alle modalità di erogazione dei servizi *cloud*, occorrerà poi, di volta in volta, scegliere la soluzione più adatta alle esigenze dell'azienda, dell'ente o del privato interessati, con un vantaggio rilevante ed intuitivo: la versatilità e l'adattabilità del servizio *case by case*.

In particolare, le valutazioni possibili possono articolarsi nella scelta tra le modalità che seguono; innanzitutto la modalità *IaaS*[13], attraverso la quale, secondo il già richiamato modello *pay per use*, vengono erogati gli strumenti

[13] Acronimo di "Infrastructure as a Service".

hardware e *software* di base[14]; quindi la modalità *SaaS*[15], spesso impiegata per le applicazioni che vengono comunemente utilizzate negli uffici in modalità *web*[16] e, in ultimo, la modalità *PaaS* [17], ossia una tipologia di servizio rivolto a operatori di mercato che lo utilizzano per sviluppare e ospitare soluzioni applicative proprie[18].

Tra i tre, il modello più comune e che ha incontrato una maggiore diffusione è il *Software as a Service* che può, perciò, considerarsi alla base dei servizi di *cloud computing;* con esso si intende qualificare una nuova concezione del *software*, svincolato dalla sua fisicità di *asset* e orientato a soddisfare le esigenze degli utilizzatori.

Emerge altresì con chiarezza come, innanzitutto, la tecnologia del *cloud computing* non faccia che rispondere in maniera più avanzata e soddisfacente alle ragioni sottostanti ai più generali processi di

[14] Come reti, capacità di elaborazione, sistemi operativi, risorse di memorie di massa, applicazioni e servizi, sono messi a disposizione del fruitore mediante *server* virtuali,

[15] Acronimo di "Software as a Service".

[16] 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.

[17] Acronimo di "Platform as a Service".

[18] Come ad esempio quelle per la gestione finanziaria, della contabilità o della logistica, per assolvere esigenze interne, oppure per fornire a loro volta servizi a terzi.

outsourcing informatico precipuamente ad uso aziendale - sui quali ci si soffermerà più innanzi - ridefinendoli e contestualizzandoli rispetto al quadro tecnologico attuale che vede un ruolo preponderante attribuito alla comunicazione *on-line*, all'interconnessione permanente fra i dipendenti delle aziende più innovative e fra le stesse ed i rispettivi clienti o fornitori, il tutto acuito dallo sviluppo su scala globale dei rapporti lavorativi e commerciali.

A ciò si aggiunga che le soluzioni *cloud* offerte dai diversi operatori possono risultare particolarmente appetibili per le piccole e medie imprese, cui vengono offerti servizi aventi lo *standard* delle grandi imprese, dei quali non potrebbero fruire se dovessero contare solamente sulle proprie risorse *in house* ma di cui hanno necessità per competere sul mercato globale. Sotto il profilo dei costi va, inoltre, tenuto conto come, nel mondo più industrializzato, quelli energetici, quelli attinenti il godimento degli immobili[19] e quelli del lavoro permangano i più significativi; da qui il vantaggio nella delocalizzazione laddove questi oneri risultino minori,

[19] I data center necessitano infatti di locali ad hoc.

senza che ciò, in ragione della concomitante diminuzione dei costi di connessione telematica, comporti particolari oneri aggiuntivi[20].

Concludendo sul punto, gli aspetti più significativi e che più di altri condizionano positivamente il ricorso all'utilizzo dei servizi di *cloud computing* emergono essere ancora una volta due e ancora una volta gli stessi: i costi molto contenuti e la comodità. L'utilizzo della tecnologia *cloud*, come già detto, consente infatti di ridurre drasticamente i costi di realizzazione e gestione di intere infrastrutture informatiche e permette altresì di semplificare le attività lavorative o di svago grazie alla possibilità di accedere ai propri dati indipendentemente dalla postazione informatica in uso e dalla posizione geografica.

[20] Cfr. A.MANTELERO, *"Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali" Saggi*, in Dir. dell'Informazione e.dell'informatica, 2010, pp.673 e ss.

.3 I profili tecnici del cloud computing e la divisione tra pubblic, private ed ibrid cloud

Prima di abbandonare l'analisi tecnica del *cloud* e di spostare definitivamente l'attenzione sulle questioni giuridiche ed esso collegate, sicuramente più interessanti data la natura di questa trattazione, è indispensabile osservare che, sotto l'aspetto tipologico prima ancora che contrattuale, rimarchevole è la distinzione, oramai consolidata, tra i tre modelli di servizio esistenti, ovvero il *Private Cloud Computing*, il *Pubblic Cloud Computing* e, da ultimo, l'*Ibrid Cloud Computing*.

Nel primo caso si fa riferimento alla realizzazione ed all'uso di un sistema di nuvole realizzato e gestito *ad hoc* per una singola azienda o per una singola Pubblica Amministrazione.

Nel caso del *Public Cloud Computing*[21], invece, ci si riferisce ad un'infrastruttura di proprietà di un fornitore, il *cloud provider*, nella quale

[21] Tipico esempio di quest'ultimo tipo di cloud è il servizio fornito per la gestione delle caselle di posta elettronica da Google e Yahoo. Con particolare riferimento ai sistemi di Public Cloud, si anticipa una riflessione importante. Bisogna rilevare che la prassi contrattuale, in questa prima fase, è stata contraddistinta dai seguenti aspetti: 1. rigidità degli accordi: l'utente non ha la possibilità di influire sui contenuti del contratto proponendo clausole o ottenendo la modifica di quelle già predisposte, potendo soltanto scegliere se aderire o meno al servizio; 2. genericità e scarsa trasparenza: salvo rare eccezioni, l'oggetto del servizio è descritto in modo generico e vengono fornite all'utente poche informazioni in

l'uso del sistema informatico non è dedicato ad un singolo utente ma ad una molteplicità di fruitori indeterminati[22].

È importante evidenziare come spesso i fruitori del servizio tendano ad optare per un modello di *cloud* privato al fine di mantenere un maggiore controllo dei dati esportati: nel *cloud* interno, infatti, questi rimangono presso le strutture organizzative su cui l'utente ha pieno ed esclusivo controllo. Adottando questo sistema, il patrimonio di dati personali e sensibili - o addirittura ultrasensibili - 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 al singolo cliente, con un inevitabile aumento dei costi.

ordine al tipo di tecnologie utilizzate, alla localizzazione dei data center, alle professionalità su cui può contare il fornitore, alle misure di sicurezza adottate; 3. poche garanzie: specialmente nei contratti rivolti ad un'utenza consumer, vi è un esonero di responsabilità pressoché totale da parte del provider che fa da contraltare alla gratuità di gran parte dei servizi forniti basti pensare, ad esempio, alla posta elettronica.

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

Per ovviare a tale inconveniente, dunque, enti, aziende e privati decidono sovente di ricorrere ad un *tertium genus*, rappresentato dal *cloud* ibrido.

Attraverso questo terzo modello è possibile demandare a un sistema di *cloud* pubblico servizi o applicazioni che coinvolgono il trattamento di dati non personali[23] o comunque non sensibili, mentre determinati processi che interessano tipologie di dati che esigono misure di sicurezza rafforzate, restano gestiti mediante il modello del *Private cloud*.

La differenziazione tipologica, lo si chiarisce subito, non è di natura meramente tecnica o terminologica; essa, piuttosto, è da ricercarsi nelle conseguenze, significative, in termini di rischi e problematiche giuridiche, sottese alla scelta dell'una tipologia di servizio piuttosto che dell'altra[24]. Nei servizi di *Public Cloud Computing*, infatti, non si ha la possibilità di negoziare i termini e le condizioni di uso, cosicché ci si trova di fronte alla scelta tra utilizzare il servizio "*as it is*" o non utilizzarlo affatto.

---

[23] Spesso trattati in modalità aggregata,

[24] Ad esempio, prendendo in esame il caso di una rete di Private Cloud, realizzata e gestita internamente, questa sarà di fatto assimilabile al tradizionale network interno e non si porranno quindi tutti i problemi legati al coinvolgimento di terzi soggetti nel trattamento dei dati immessi.

Al contrario, nell'utilizzo di un sistema di *Private Cloud Computing* si ha più spesso la possibilità di negoziare il contratto di servizio che regolerà il rapporto tra l'utilizzatore ed il *provider*.

Al momento attuale, data la loro intuibile maggiore utilità, le soluzioni di *public cloud* sono quelle di maggiore uso per via della loro forte scalabilità. Rispetto a questo contesto, pare quindi necessario interrogarsi in ordine a quella che è la qualificazione giuridica del soggetto che rivestirà il ruolo di *cloud provider*, vero e proprio gestore e perciò conoscitore e custode dei dati immessi *in the cloud*, in ragione della natura e delle modalità con cui la prestazione verrà offerta .

CAPITOLO SECONDO

I CONTRATTI DI CLOUD COMPUTING

Sommario: *1. I servizi di cloud computing e il problema dell'inquadramento contrattuale; 1.2 La struttura del contratto di cloud; 1.3 Lo schema "per adesione"; 1.4 "Accesso" al servizio o "Erogazione" del servizio? – 2. La qualificazione giuridica del contratto di cloud a metà tra l'atipicità dell'elemento causale e il negozio "misto" - 3. Contratti di cloud ed outsourcing.*

.1 I servizi di cloud computing e il problema dell'inquadramento contrattuale

Col primo Capitolo si è tentato d'introdurre, attraverso una preventiva analisi strutturale dell'oggetto del presente lavoro, quella che da qui innanzi sarà la trattazione del *cloud computing* dalla prospettiva che risulta di maggiore interesse in questa sede: l'approccio giuridico.

Fin ora infatti, si è cercato di delineare le sole caratteristiche più che altro tecniche del fenomeno *cloud*, spiegando innanzitutto l'utilità e le finalità del servizio; nulla ancora però si è detto sulle implicazioni giuridiche più rilevanti riconnesse all'utilizzo su larga scala di questa nuova tecnologia.

Ebbene, si preciserà subito che tali implicazioni sono innumerevoli e anche assai significative; probabilmente anzi, non pare esagerato affermare che, da quando esiste l'informatica, mai nessuna nuova tecnologica ha avuto implicazioni di natura giuridica così rilevanti come il *cloud computing*.

Ciò eminentemente per un motivo: attraverso l'utilizzo dei servizi di *cloud* la *privacy* degli utenti, ma anche la sicurezza dei dati immessi *in the cloud,* sono sottoposti a dura prova.

Tuttavia, prima di allargare l'orizzonte della trattazione a queste tematiche e una volta capito quando, effettivamente, si possa discorrere di servizi importati e offerti "da e sulla nuvola", è preliminarmente opportuno soffermare la nostra attenzione sull'aspetto contrattuale del servizio, ovvero sulla natura della relazione che legherà, di volta in volta, gli utenti-fruitori dei servizi di *cloud* e gli erogatori degli stessi, i già più volte richiamati *cloud providers.*

Il passaggio è di cruciale importanza; dall'analisi di tale relazione negoziale dipendono, infatti, una miriade di conseguenze quali la

corretta qualificazione giuridica del contratto stipulato, la determinazione della disciplina e della legge ad esso applicabile e l'individuazione delle clausole contrattuali più importanti su cui perciò dovrà focalizzarsi maggiormente l'attenzione delle parti[25].

La contestualizzazione del rapporto contrattuale *user - cloud provider* diventa oltremodo complessa se si considera che i più importanti operatori del settore *cloud* sono quasi tutti statunitensi, con l'ovvia conseguenza pratica che, indipendentemente da questioni ulteriori connesse alla individuazione della legge applicabile, i contratti da questi approntati vengono per la quasi totalità redatti in lingua inglese[26]; non sarà sempre dato, pertanto, rinvenire una categoria ed una terminologia giuridica univoca e corrispondente, di volta in volta, in maniera precisa alle categorie ed alle terminologie giuridiche degli ordinamenti di appartenenza dei singoli clienti, con evidenti potenziali problemi di confusione circa il tipo di

[25] Cfr. E.BELISARIO, *"Cloud Computing" , Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011, pag. 11 e ss.

[26] Per quanto concerne l'esperienza italiana, solo di recentissimo si sono riscontrati dei tentativi di traduzione, anche piuttosto dozzinali, che tuttavia non implicano necessariamente un adeguamento, oltre che linguistico, anche concettuale.

contratto che ci si accinge effettivamente a concludere ovvero sui servizi che con esso effettivamente si vanno ad acquistare.

Si aggiunga che i contratti di *cloud computing* sono immateriali; nella maggioranza dei casi, essi, infatti, vengono conclusi interamente *on-line*, bypassando in modo pressoché assoluto la fase delle trattative e riducendosi il peso decisionale dell'utente ad un semplice processo di adesione a moduli o formulari predisposti dal solo *cloud provider*, resi disponibili sul sito internet dello stesso fornitore.

1.2 Lo schema "per adesione"

Nell'ipotesi italiana, comune tra l'altro a molte esperienze degli altri ordinamenti dell'area *civil*, la tipologia contrattuale appena descritta rientra tra quella che dottrina e giurisprudenza maggioritarie definiscono "contrattazione conclusa mediante l'uso di strumenti informatici", a sua volta sussumibile nel più ampio *genus* dei contratti per adesione conclusi al di fuori dei locali commerciali.

Tale tipologia contrattuale incontra un regime giuridico di marcata tutela della parte debole del contratto, ovvero il consumatore - che nel nostro caso diventa un consumatore "qualificato": è l'utente *cloud* - il quale, come appena osservato, data l'assenza della fase delle trattative vedrà il suo ruolo contrattuale ridotto alla mera valutazione circa l'opportunità o meno di aderire alle offerte predisposte dal fornitore.

Questa circostanza può determinare, e molto spesso determina, un significativo squilibrio tra le parti con una netta soccombenza dell'utente, acuita tutte le volte in cui i servizi offerti rientrino nell'alveo del *Public Cloud*, per il quale è assolutamente escluso anche il benché minimo spiraglio di contrattazione tra le parti. E la soccombenza diventa ben più significativa quando, tra le clausole contrattuali predisposte unilateralmente dal solo fornitore del servizio, siano presenti le così dette clausole vessatorie[27].

[27] Si pensi ad esempio alle clausole – vessatorie – con le quali venga predisposto l'esonero da responsabilità o una forte riduzione della responsabilità del *cloud provider* per eventuali danni, perdite o accessi di terzi ai dati archiviati, limitative in ordine alla possibilità di recesso, ovvero alla deroga del foro competente per eventuali controversie.

Prendendo in esame - per questioni più che altro di comodità geografica - l'esperienza italiana, tra l'altro abbastanza simile a quella francese e tedesca, al fine di valutare la sorte delle clausole in questione è opportuno distinguere i casi in cui l'utente di servizi *cloud* sia un consumatore da quelli in cui l'utente sia invece un'impresa o un professionista.

Nel primo caso vengono in rilievo le disposizioni dettate dal D.Lgs. n. 206/2005. In base all'art. 33 del decreto, infatti, si considerano vessatorie le clausole che, malgrado la buona fede, determinano a carico del consumatore un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto. Al fine di agevolare l'opera dell'interprete, il Legislatore ha individuato una serie di clausole che - fino a prova contraria - si presumono vessatorie[28].

La definizione, per quanto chiara, crea molti dubbi interpretativi, particolarmente in ordine al significato della locuzione " malgrado la buona fede".

[28] Cfr. E.BELISARIO, "*Cloud Computing" , Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011, pag. 15 e ss.

L'ottica comparatistica alla quale il presente lavoro costantemente tende ad indirizzarsi non può non portarci ad osservare la situazione così così come si presenta oltr'Alpe; nell'esperienza francese e in quella inglese, ad esempio, il riferimento alla buona fede è in senso "oggettivo" ovvero quale criterio di "correttezza" cui deve essere improntato l'intero contenuto dell'atto e tutta l'attività negoziale. Il nostro legislatore ha invece preferito una qualificazione in senso "soggettivo" della buona fede, intesa, diversamente dalle accezioni appena richiamate, quale ignoranza di ledere un altrui diritto.

Una volta tanto, la soluzione nazionale pare migliore e più all'avanguardia delle altre; ciò perché innalza la soglia di tutela del consumatore italiano rispetto alla media europea, assunto che basti l'oggettiva creazione di uno squilibrio tra i soggetti contrattuali per vedersi riconosciuta la posizione di favore, indipendentemente dalla esistenza o meno della malafede da parte del professionista.

In questo contesto, perché una clausola possa dirsi vessatoria deve dar luogo ad uno squilibrio innanzitutto normativo più che economico in quanto

la effettiva convenienza o meno, nella fattispecie, di un contratto di *cloud*, non può mai essere rimessa al sindacato del giudice, costituendo oggetto di insindacabile decisione delle parti[29].

Nel caso in cui nel contratto siano presenti tali clausole, queste sono da considerarsi, secondo la prassi normativa, nulle, mentre l'accordo rimane valido per il resto; l'unica possibilità per evitare la loro nullità è renderle oggetto di trattativa individuale.

E' questo un passaggio assai significativo e problematico in ordine ai contratti di *cloud*; ciò perché, come osservato, la prassi contrattuale affermatasi in materia di *cloud computing* non prevede quasi mai la possibilità di una negoziazione o di una trattativa individuale. Si pensi alle ipotesi di *Pubblic Cloud*; in questo caso viene meno la stessa sottoscrizione in quanto l'adesione avviene quasi sempre mediante registrazione dell'utente sul sito del *provider*.

Quando l'utente del servizio *cloud* non sia un consumatore semplice troverà applicazione la disciplina dettata dagli artt. 1341 e ss.

---

[29] Cfr. E.BELISARIO,*"Cloud Computing" , Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011, pag. 15 e ss

del codice civile, con una variazione, tuttavia, quasi insignificante in termini pratici. L'art. 1341 c.c. prevede che nei c.d. "contratti standardizzati" le condizioni generali siano efficaci nei confronti della parte non predisponente a condizione che quest'ultima le abbia conosciute o, quanto meno, abbia avuto la oggettiva possibilità di conoscerle utilizzando l'ordinaria diligenza, in virtù del principio del c.d. "agire informato"; tuttavia, al comma successivo dello stesso articolo vi è la previsione secondo la quale, nel caso in cui nel contratto siano state predisposte delle condizioni generali che realizzino a carico di una parte e a favore dell'altra un significativo squilibrio dei diritti e degli obblighi discendenti dall'accordo negoziale, queste siano inefficaci e siano espunte dal contenuto del contratto salvo che non siano "specificamente approvate per iscritto".

Ancora una volta, il legislatore privilegia l'interesse del soggetto aderente che non ha interagito volitivamente alla stipulazione del contenuto negoziale.

E allora*, quid iuris* per le clausole vessatorie contenute in un contratto concluso con il mezzo telematico, dove, evidentemente, manca in modo assoluto la possibilità della materiale sottoscrizione?

Ci si è posti, così, l'interrogativo circa l'idoneità della tecnica del *"doppio click"* e se quindi questa strategia possa considerarsi idonea a configurare una specifica approvazione delle clausole che implicano la sproporzione, in modo da soppiantare l'onere dell'apposizione della doppia firma in questa situazione evidentemente impossibile; la dottrina e la giurisprudenza maggioritarie, comuni anche a molti altri sistemi dell'area *civil*, si sono pronunciate sfavorevolmente rispetto a questa scorciatoia, non ritenendola idonea a conferire validità alle clausole vessatorie per l'efficacia delle quali si riterrebbe sempre indispensabile una effettiva sottoscrizione, sia pure in formato elettronico; ciò perché solo la firma, a differenza delle altre forme di manifestazione della volontà, si considererebbe idonea a tutelare nel miglior modo possibile l'interesse dell'aderente.

Nella prassi italiana si è ritenuto in tempi piuttosto recenti di potere proporre una interpretazione in senso evolutivo dello stesso art. 1341 c.c., ampliando il concetto di firma anche a quella digitale. Tale interpretazione evolutiva è atto dovuto, nel senso che la specifica approvazione per iscritto era prevista dal legislatore del 42' perché all'epoca prevalente era indubbiamente la forma scritta dei contratti. Oggi la realizzazione di contratti in forma cartacea può considerarsi oramai residuale e pressoché desueta, essendo essa stata sostituita, a seguito della pressante evoluzione tecnologica, dalla stipulazione degli stessi per via telematica, data la sua duttilità, la maggiore velocità ma anche per i costi molto più contenuti.

In secondo luogo, poiché la finalità della "specifica approvazione per iscritto" segue la logica di consentire al contraente di valutare in modo più attento e ponderare la possibilità di concludere un contratto contenente pattuizioni per lo stesso particolarmente onerose, detta finalità, oggi, può essere ampiamente soddisfatta con il cd. "*doppio click*", purché l'aderente sia messo nella concreta possibilità di conoscere, senza confusione o modalità fuorvianti, il concreto contenuto delle condizioni generali inserite

nel contratto. Questo comporterebbe un maggiore onere a carico dei *cloud provider:* rendere semplice all'altro contraente il contenuto dei contratti, accentuandone in modo esponenziale la chiarezza, vista anche la distanza e l'asimmetria informativa che separa le parti[30].

1.3 "accesso" al servizio o "erogazione" del servizio?

Come già accennato in precedenza, l'elemento peculiare del *cloud* è l'erogazione di un servizio.

Non a caso, le tipologie di prestazione dei servizi di *cloud* sono tutte caratterizzate dalla locuzione *"as a service": "software as a service"," platform as a service"," infrastructure as a service"*[31].

Questa connotazione è giuridicamente rilevante, poiché ribalta il tradizionale modello *lato sensu* proprietario della gestione delle risorse informatiche, non solo in ambito privato quanto soprattutto in ambito aziendale, in cui si era soliti avere un controllo ed una gestione diretti sulle stesse.

---

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

[31] Cfr. A.MANTELERO, *"Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali" Saggi*, in Dir. Informaz.informat., 2010, pp.682 e ss.

Essendo, invece, il *cloud* un modello incentrato sull'erogazione di servizi da parte di terzi fornitori, l'informatica si troverà, adesso, ad uscire uscire dall'azienda per poi essere ad essa restituita mediante un meccanismo meccanismo basato sulla possibilità di accesso ad alla stessa[32].

Ciò posto, tanto nella letteratura giuridico-economica quanto in quella sociologica, si parla oggi di "cultura dell'accesso"[33], dove l'importante non è più essere proprietari della risorsa bensì essere in condizioni di poter accedere ad essa grazie all'operato svolto, in tal senso, da terzi che la detengono e la erogano.

Dal punto di vista contrattuale tale mutamento di paradigma è tanto determinante quanto fondamentale. Se, infatti, il servizio diviene centrale, aumenterà l'importanza assunta dal contratto che quel servizio è destinato a disciplinare nel tempo; se la disponibilità delle risorse dipende da terze parti, occorre che queste assicurino la continuità della prestazione e la

[32] L'idea dell'informatica come servizio, anziche´ come bene, e` risalente nella sua elaborazione teorica, cfr. D.F. PARKHILL, *The Challenge of the Computer Utility,* Reading Mass., 1966.
[33] H.RIFKIN, *L'era dell'accesso*, Milano, 2000 e, con specifico riferimento ai servizi di cloud computing, SUN MICROSYSTEMS, *Introduction to the Cloud Computing Architecture, White Paper*, *1st Edition,* giugno 2009, in *http://webobjects.cdw.com* ed INTERNATIONAL TELECOMMUNICATION UNION, *Distributed Computing: Utilities, Grid & Clouds*, 2009, in *www.itu.int*.

cooperazione fra fornitore ed utilizzatore; serve, quindi, un'attenta e puntuale regolamentazione del rapporto[34].

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

.2 La qualificazione giuridica del contratto di cloud a metà tra l'atipicità dell'elemento causale e il negozio "misto"

Sotto il profilo della più stretta qualificazione giuridica, per la quasi quasi totalità degli studiosi di settore la pluralità degli accordi su cui si appoggia l'erogazione dei servizi di *cloud computing* avrebbero natura di contratti misti, in quanto, in essi, verrebbero a coesistere elementi riconducibili tanto all'appalto di servizi quanto al contratto di licenza[35].

Nella fattispecie, infatti, il contratto di *cloud* non si presenta con una struttura sua propria ma si costituisce attraverso il ricorso a due diversi schemi negoziali tipici e precisamente: l'appalto di servizi e il contratto di licenza[36].

Nel quasi totale disinteresse della giurisprudenza, non solo di casa nostra ma anche internazionale, in ordine all'argomento la dottrina si è più o

---

[35] Cfr. A. MANTELERO nella relazione: *"Il cloud computing; inquadramenti giuridici e differenze di approccio contrattuale"* tenuta dall'autore al convegno di Milano del 17 gennaio 2012 *:"Cloud Computing - I diversi approcci contrattuali e nuove definizioni in ambito privacy"*. L'audio di tale intervento e la relativa presentazione sono fruibili on-line.

[36] Diverse le tesi in ordine alla natura del contratto di Cloud. Sull'argomento cfr.: S.BENDANI, *Software as a Service (Saas): aspetti giuridici e negoziali, in http://www.altalex.com/index.php?idnot=44076;* N.FABIANO, *I nuovi paradigmi della rete. Distribueted computing, cloud computing e "computing paradigms":abstract sugli aspetti e profile giuridici*, *in http://www.diritto.it/art.php?file=/archivio/27973.html.*

meno equamente divisa tra i due orientamenti. Tuttavia, la tesi al momento maggiormente condivisibile[37] parrebbe essere quella di chi ritiene il contratto di *cloud* - tanto di *Public* quanto di *Private* - assimilabile allo schema dell'appalto di servizi; ciò con particolare riferimento ai sistemi di *cloud computing* di tipologia *SaaS*[38] .

Pare quindi necessaria una disamina di entrambe le contrapposte teorie, al fine di una loro migliore comprensione.

Notoriamente, l'appalto di servizi, partendo dalla definizione che di esso ci offre il nostro codice civili all'art. 1665[39], consiste in un *facere*, quindi nella prestazione di un'attività che si realizza nell'obbligo, in capo all'appaltatore, di fornire un servizio a fronte di un corrispettivo predeterminato, in accordo con il committente; nei contratti di *cloud*, tale obbligo si concretizzerà precipuamente nell'offerta di memorie di massa ed altri servizi.

---

[37] S. BENDANDI, *Software as a Service (SaaS): aspetti giuridici e negoziali*, in http://www.altalex.com/index.php?idnot=44076

[38] Abbreviazione di Software as a Service; riconducibili - lo si anticipa – più delle atre tipologie, al fenomeno dell'outsourcing, del quale si parlerà a breve.

[39] Testualmente: " il contratto col quale una parte assume, con organizzazione dei mezzi necessari e con gestione a proprio rischio, il compimento di una opera o di un servizio verso un corrispettivo in danaro".

La sussunzione del *cloud* tipologia *SaaS* in questa norma, è parsa ai più pressoché lapalissiana; nel *Software as a Service* infatti, la caratteristica principale, come già accennato, è data proprio dallo sfruttamento di una struttura informatica esterna rispetto a quella privata o aziendale , al fine della fruizione di servizi *software* gestiti , di fatto, da terzi[40].

Ciò posto, secondo quest'orientamento interpretativo, ed esaminando quali siano effettivamente le prestazioni che vengono di volta in volta erogate nell'esecuzione di un contratto di *cloud*, emergerebbe nelle stesse la prevalenza di una prestazione di fare; quest'ultima, essendo data dalla fornitura di alcuni servizi *software* da parte del fornito che utilizza mezzi propri a fronte del pagamento di un corrispettivo, farebbe propendere per l'inquadramento del contratto nella tipologia dell'appalto di servizi, sia pure nelle ipotesi in cui esso abbia ad oggetto - quasi sempre - prestazioni continuative o periodiche[41].

---

[40] In particolare, lo si anticipa, questa tipologia di cloud viene ricondotta all'outsourcing proprio in relazione alla circostanza per cui si affida a terzi la gestione di quella che sarebbe stata in loco una vera e propria infrastruttura informatica.

[41] Cfr. E.BELISARIO , *" Cloud Computing" , Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011 pp. 11 e ss

L'inquadramento nel contratto di appalto di servizi ha, ovviamente, alcune specifiche conseguenze: in particolare, l'obbligazione assunta dall'appaltatore dovrà essere considerata, irritrattabilmente, di risultato; non dovrà, quindi, trarre in inganno la circostanza per cui il fornitore, a corollario del servizio offerto al proprio cliente, sia chiamato, necessariamente, a supportare tutte le attività ed i processi di *business* della propria organizzazione per garantire tutti gli aspetti relativi alla sicurezza ed alla *privacy* dei dati, alla continuità del servizio, eccetera[42].

Il contratto di licenza invece, anche detto contratto d'uso, è uno strumento legale che può accompagnare, consentendone l'utilizzo, un prodotto, molto spesso un programma informatico, specificando proprio le modalità con cui l'utente può utilizzare e ridistribuire tale prodotto, garantendo dei diritti ed imponendo obblighi o vincoli.

Nel nostro caso, si ha il richiamo alla licenza tutte le volte in cui il servizio di *cloud* si sostanzi nell'offerta di *software* e nel loro conseguente utilizzo da parte dei fruitori.

[42] E. BELISARIO, *op.cit.*

Optare drasticamente per la riconduzione ad una figura negoziale piuttosto che a un'altra è parso assolutamente insoddisfacente; ecco perché sembra più corretto ritenere che il contratto di *cloud* sia un contratto atipico o meglio ancora misto. Ciò in quanto esso ricorre, in maniera variabile, ad elementi peculiari tipici tanto dello schema dell'appalto quanto a quello della licenza. Nella redazione concreta dei loro contratti infatti, i vari fornitori oscilleranno, di volta in volta, fra queste due figure negoziali, dando, a seconda dei casi, maggiore spazio alle componenti riconducibile all'uno piuttosto che all'altro modello.

Ma la licenza e l'appalto non sono gli unici modelli di riferimento nella stipulazione dei contratti di *cloud*.

Altra parte della dottrina, infatti, seppur minoritaria, ha fortemente osteggiato la sussunzione del negozio tanto nello schema dell'appalto di servizi quanto in quello della licenza, sostenendo a più voci che si tratterebbe di uno schema negoziale puramente e prettamente atipico, sotto tutti i punti di vista, anche in ottica consequenziale e rimediale.

Tale orientamento si basa sulla considerazione secondo la quale i servizi di tipo *SaaS* non vengono realizzati di volta in volta per i singoli utenti ma questi ultimi si limitano ad utilizzare servizi già precedentemente realizzati; in quest'ottica, ciò sarebbe sufficiente ad escludere che il contratto di *cloud computing* possa essere ricondotto tanto alla categoria dell'appalto di servizi quanto a quella della licenza.

A sostegno della atipicità dei contratti di questo tipo, viene fatto riferimento proprio alle caratteristiche salienti dei sistemi di *cloud* come quelli relativi all'accesso al servizio in base alle esigenze di chi lo usa, alla possibilità di raggiungerlo e sfruttarlo da una qualsiasi postazione informatica collegata ad internet, alla flessibilità ed in genere a tutte quelle caratteristiche che abbiamo definito sin dall'inizio come elementi positivi di questa nuova tecnologia[43].

[43] E. BELISARIO, *op. cit.*

Tra le tre, la tesi più ampiamente seguita[44] e sicuramente considerata maggiormente condivisibile risulta essere quella che riconduce il contratto per la erogazione dei servizi di *cloud computing* - siano essi di tipo pubblico, ibrido o privato – allo schema dell'appalto di servizi. Ciò innanzitutto in considerazione delle modalità attraverso le quali si realizza la stessa offerta del servizio, ma anche e soprattutto in ragione della riconducibilità della fattispecie, da tempo nella prassi prima ancora che in termini di riconoscimento giuridico, allo schema dell'*outsourcing* informatico.

Ad una attenta osservazione dello schema contrattuale, infatti, si comprenderà facilmente come la prestazione oggetto dell'accordo che intercorre, di volta in volta, tra il fruitore e l'erogatore del servizio, sia rappresentata dall'obbligo di conservazione e gestione, del secondo in favore del primo, di una parte del sistema informativo, che dovrà perciò essere dedicata esclusivamente al singolo cliente. Da ciò non si può non constatare come il nucleo essenziale di quella prestazione sia riconducibile

[44] Tanto in dottrina, che sull'argomento si sta affacciando solo in tempi soltanto recentissimi, tanto nella primordiale giurisprudenza che con intense e difficili ricerche è dato rinvenire.

alla figura contrattuale che, almeno nell'ordinamento italiano, viene definita e disciplinata appalto di servizi.

Tale conclusione è suffragata da ulteriori considerazioni di fatto.

In primo luogo, l'utilizzazione di un sistema di *cloud computing* prevede l'affidamento a terzi di una o più attività che hanno ad oggetto determinate operazioni informatiche; ne deriva che la natura dell'attività svolta dal medesimo provider presuppone l'esistenza di una vera e propria organizzazione di impresa senza la quale non sarebbe gestibile un sistema basato sulle nuvole[45].

Ulteriore elemento di apicale importanza in termini di propensione a favore della tesi del contratto d'appalto di servizi è rintracciabile nell'assunzione dell'intero rischio contrattuale da parte del fornitore; il fornitore della nuvola, infatti, è obbligato ad accollarsi i rischi derivanti dalla gestione della struttura informatica messa a disposizione dei clienti e, sebbene con i dovuti limiti, risponderà nei loro confronti allorquando dovesse realizzarsi il mancato

[45] E. BELISARIO, *op. cit.*; Si pensi, a mero titolo di esempio, alla struttura informatica necessaria a gestire servizi integrati di posta elettronica, produzione documentale e memorizzazione di dati e a come la stessa richieda risorse hardware e software particolarmente complesse.

raggiungimento del risultato contrattualmente previsto, il tutto nei termini e con le modalità stabilite nei livelli minimi di servizio, laddove questi ultimi siano stati previsti e dei quali meglio si dirà più innanzi.

E allora, da tutto quanto sin qui detto, si può concludere che, almeno per quanto concerne l'esperienza italiana, il contratto di *cloud*, salvo casi particolari, è in via generale riconducibile alla categoria dell'appalto di servizi, disciplinato dagli articoli 1655 e ss. del nostro codice civile, potendo perciò, al limite, addirittura considerarlo un contratto tipico.

Tuttavia, stante nella pratica l'assenza di un profilo contrattuale di fatto prevalente, registrandosi piuttosto l'alternanza tra situazioni in cui prevale la struttura del contratto di servizio e schemi in cui prevale quello di licenza, pare più opportuno e preciso considerare i contratti di *cloud* dei contratti misti dal punto di vista dell'elemento causale. Non si può però trascurare un altro, importante accostamento: quello all'*outsourcing*.

3. *Contratti di cloud ed outsourcing*

Nei paragrafi precedenti e nell'intero corso di tutto questo secondo capitolo, più volte si è fatto riferimento ad un concetto che si rivelerà di estrema importanza nell'ottica della giusta qualificazione del contratto sotteso alla erogazione dei servizi di *cloud computing*; l'*outsourcing*.

L'*outsourcing* nasce come un concetto di matrice prettamente aziendale[46] e la correlazione, nonché la sua strettissima attinenza, col fenomeno *cloud* deriva proprio dalla vasta applicazione che di questa tecnologia si sta facendo, sin dal suo esordio, proprio nel contesto aziendale.

Con questo termine si suole indicare il processo attraverso il quale una o più attività dell'impresa vengono portate fuori ovvero affidate a terzi soggetti che svolgono la propria opera lavorativa al di fuori dell'azienda e che non sono parti del circuito aziendale, con un

[46] Per eventuali approfondimenti: R.H. COAST, *The Nature of the firm*, in Economica, vol.4, n.16, 1937, 386 ss.; O.E WILLIAMSON, *Markets and Hierarcjies; Analysis and Anti-Trust Implication*, New York, 1975; U.ARNOLD, *New dimensions of outsourcing: a combination of transaction cost economics ande the core competencies concept*, in European Journal of Purchasing & Supply Management, n. 6 (1), 2000, pp. 23 e ss.

conseguente, significativo, mutamento in termini strutturali ed evidenti implicazioni, *icto oculi,* di carattere tanto strategico quanto organizzativo e organizzativo e di controllo dei processi e delle dinamiche produttive nonché delle più generali informazioni inerenti la vita dell'azienda stessa[47].

In altre parole, con il termine *outsourcing* si intende fare riferimento al c.d. fenomeno della "esternalizzazione", il processo in virtù del quale alcune attività produttive - generalmente quelle d'importanza e caratura minore - vengono affidate alla cura ed alla gestione di soggetti terzi rispetto all'azienda e ad essa non appartenenti[48]. Tutto ciò al fine di recuperare risorse in favore dei rami più impegnativi e profittevoli dell'impresa, potendo comunque continuare a fruire dei risultati delle attività

[47] Ciò in quanto si realizza un vero e proprio passaggio da un controllo diretto ed interno di tutti gli aspetti della vita dell'azienda ad un modello di gestione della stessa decentrato, costituito in prevalenza dal ricorso a strumenti di natura contrattuale.

[48] In tal senso A.MANTELERO, *Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali, Saggi*, in Dir. Dell'Informazione e dell'informatica., 2010, pp. 674 e ss. E ` questo il modello di outsourcing (c.d. direct third party outsourcing) che qui interessa, poiche´ ad esso fanno principalmente riferimento le operazioni che vedono il ricorso al cloud computing, mentre non verranno considerati gli altri modelli in cui si prevede la creazione di un'unita`operativa all'estero da parte di una societa` madre (captive direct) o in cui si da` vita ad una joint venture con la societa` estera outsourcee. Con riferimento ai processi di outsourcing nel settore ICT in generale, oltre che al cloud computing, cfr. anche POLITECNICO DI MILANO – DIP. D'INGEGNERIA GESTIONALE, *ICT Strategic Sourcing: nuovi equilibri oltre la crisi; Rapporto 2009 Osservatorio ICT Strategic Sourcing*, novembre 2009,http://www.osservatori.net/ict_strategic_sourcing/rapporti/rapporto/journal_content/56_INSTANCE_0HsI/10402/574901.

esternalizzate, ricevendoli dagli *outsourcee* sotto forma di prestazioni di servizi.

L'attribuzione di compiti e fette di produzione a realtà aziendali esterne, che incentrano il loro *business* su questa tipologia di servizi, implica un grandissimo vantaggio, ovvero una riduzione dei costi che traduce, poi, in un contenimento del prezzo che *l'outsourcer* viene a per fruire dei servizi che esso stesso ha deciso di esternalizzare rispetto costo che avrebbe invece dovuto sopportare se avesse perpetrato la gestione *in house* di quelle stesse attività.

Nell'ipotesi, frequente, di esternalizzazione di attività di natura informatica - l'ICT - il vantaggio è addirittura doppio, perché l'*outsourcer* risparmierà tutti i costi correlati alla gestione del rischio connaturato a questa tipologia di attività.

L'assonanza tra i processi di *outsourcing*, così come brevemente descritti, e i servizi di *cloud computing* è evidente; anzi, molto spesso le aziende realizzano i processi di *outsourcing* informatico proprio avvalendosi della tecnologia del *cloud computing*.

Evidente è, altresì, la similitudine tra gli schemi contrattuali impiegati per l'erogazione dei servizi di *cloud computing* in ambito aziendale e l'*outsourcing* senza trascurare, tuttavia, gl'importanti elementi di differenziazione[49].

Anche l'*outsourcing*, come il *cloud computing*, non costituisce una tipologia contrattuale tipica[50]; esso, piuttosto, prende vita attraverso l'utilizzo di una pluralità di fattispecie eterogenee, anche queste tutte in gran parte riconducibili all'appalto di servizi, che qui, però, diverrà, "qualificato" perché specificamente indirizzato alla regolamentazione dei processi di esternalizzazione di fette di produzioni aziendali[51].

---

[49] Cfr. A. MANTELERO , *Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali, Saggi*, in Dir. dell'Informazione e dell'Informatica., 2010, pp.682 e ss.

[50] In dottrina si sottolinea come l'outsourcing rilevi sotto il profilo funzionale ed organizzativo e non in quanto modello contrattuale o categoria giuridica autonoma; cfr. F. CARDARELLI, *La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing,* in Dir. dell'Infirmazione e dell' Informatica, 1993, I, 86, secondo cui tale termine « non puo` avere alcuna rilevanza giuridica »; cosı` anche M. PITTALIS, *Outsourcing,* in Contr. e impr., 2000, pp. 1006 e ss. Con riguardo al profilo contrattuale inerente la gestione del processo di outsourcing informatico si vedano: F. TOSI, *Il contratto di outsourcing di sistema informatico*, Milano, 2001; M. PITTALIS, op. cit., pp. 1010 ss.; A. MUSELLA, *Il contratto di outsourcing del sistema informativo*, in Dir. dell' Informazione e dell'Informatica, 1998, pp. 857 e ss..

[51] Sebbene i processi di esternalizzazione vengano regolati fra le parti facendo ricorso ad una varietà di modelli contrattuali, per quanto concerne, invece, l'acquisizione del servizio erogato dall'outsourcee, il rapporto sussistente fra le parti risulta solitamente riconducibile al contratto di appalto di servizi,come spesso avviene anche nelle ipotesi di cloud compuring. Cfr. in dottrina: O. CAGNASCO – G. COTTINO, *Contratti commerciali*, in *Trattato di Diritto Commerciale* diretto da G. COTTINO, Padova, 2000, p. 353;

Fra i punti comuni ai due modelli, innanzitutto vi è una chiara analogia di scopo, data dalla esternalizzazione di parte di servizi o attività, quindi la redazione del contratto in funzione della centralità del servizio e della qualità dello stesso; da qui l'attenzione, presente in entrambe le fattispecie, per la definizione di specifici *standard* inerenti le prestazioni, per la predisposizione di indici e parametri atti a misurare l'efficienza del servizio, nonché per la definizione delle metriche di costo, anche in ragione di tali indicatori.

La necessità di regolare in maniera analitica tali profili comporta, sul piano della forma contrattuale, una certa complessità strutturale dei contratti di *cloud computing*, in cui il documento contenente gli elementi fondamentali dell'accordo viene ad essere affiancato da tutta una serie di allegati tecnici, che definiscono nel dettaglio i vari parametri del servizio, assicurando, in tal modo, l'impegno della parte fornitrice circa la qualità della prestazione.

M. PITTALIS, *Outsourcing*, cit., p. 1015 ss.; A. MUSELLA, *Il contratto di outsourcing del sistema informativo*, cit., pp. 859 ss.; F. CARDARELLI, *La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing*, cit., p. 94.

Le divergenze rispetto ai modelli contrattuali che regolamentano i processi di *outsourcing* sono, invece, in primo luogo riscontrabili nel fatto che, mediante questi ultimi, non si realizza solamente un'esternalizzazione delle risorse strutturali ma anche delle così dette risorse umane. Analoghe soluzioni organizzative si riscontrano, invece, con difficoltà e sono comunque fortemente ridotte nei servizi di *cloud computing*, laddove simili esigenze risultano minimizzate dalla netta prevalenza dei profili inerenti l'organizzazione di mezzi e strutture rispetto alla dotazione di personale.

Ulteriore elemento distintivo è dato dal fatto che, particolarmente nel modello del *Pubblic cloud computing,* lo schema contrattuale si basa su modelli di erogazione "uno a molti"[52]; i contratti sono perciò per lo più standardizzati e destinati ad un'ampia platea di soggetti[53].

[52] Cfr.A.MANTELERO , nella relazione su "*Cloud computing e pubblica amministrazione: criticità e vantaggi"* , nell'ambito del convegno "*Public Private Cloud*" svoltosi il 28 giugno 2011 a Pontecchio Marconi, Bologna.

[53] Tale uniformità, lo si sottolinea, si rende necessaria in presenza dell'offerta di un servizio standardizzato, rispetto al quale non sarebbe efficiente declinare in maniera personalizzata le modalità dello stesso ed anzi, per sua natura, richiede che vengano predefiniti a monte criteri uniformi.

Nell'*outsourcing* tradizionale, invece, si è solitamente in presenza di un rapporto molto forte fra le parti, sovente caratterizzato anche da vincoli di esclusiva, in un contesto, tra l'altro, in cui il servizio è molto personalizzato in ragione delle esigenze del cliente.

Nel caso del *cloud computing* , come già più volte detto, le prestazioni erogate sono standardizzate perché destinate ad un'ampia platea di soggetti.

La distinzione nel modello di offerta è, poi, destinata a riverberarsi sul piano contrattuale sin dal momento che precede la stipulazione dell'accordo, necessariamente più lunga ed articolata nel caso dell'*outsourcing*, più breve, anzi quasi inesistente, nel caso del *cloud computing,* proprio in ragione della standardizzazione delle prestazioni offerte[54].

A mutare, perciò, sarà pure la dinamica negoziale, poiché mentre i prodotti *cloud* vengono disciplinati attraverso contratti *standard* non negoziati, nell'*outsourcing*, in virtù della personalizzazione del

[54] Cfr. A.MANTELERO, *Il contratto per l'erogazione alle imprese di servizi di Cloud Computing*, *Saggi*, in Contratto e Impresa 4-5/2012, disponibile on-line all'indirizzo http://ssrn.com/abstract=2142050

servizio, il contratto è oggetto di negoziazione in ogni sua singola clausola.

In ultimo, la peculiarità dei servizi richiesti dal cliente che connota le operazioni di *outsourcing* comporta una metrica dei costi assai più complicata che dovrà tenere conto, di volta in volta, delle specifiche richieste avanzate dall'*outsourcer,* mentre nei contratti di *cloud* la standardizzazione dei contratti corrisponde ad una standardizzazione anche dei costi e ad una loro estrema semplificazione, incentrata su alcuni parametri di base quali la frequenza di utilizzo, la quantità delle risorse impiegate e la durata dell'impiego[55].

Le aziende sono ormai fortemente proiettate verso la realizzazione di processi di *outsourcing* informatico attraverso l'utilizzazione della tecnologia del *cloud computing*; sfruttando le potenzialità della comunicazione a distanza, attraverso le reti telematiche, è infatti possibile concentrare in grandi *data center* le risorse informatiche di più aziende, con una economizzazione dei costi ed una comodità della quale si è già abbondantemente discusso. E' evidente come il *cloud* non faccia che rispondere in maniera più avanzata e soddisfacente alle ragioni sottostanti ai

[55] Cfr. A. MANTELERO, *op. cit.*

più generali processi dell'*outsourcing* informatico, ridefinendole e contestualizzandole rispetto al quadro tecnologico attuale che vede un ruolo preponderante attribuito alla comunicazione *on-line*, all'interconnessione permanente fra i dipendenti delle aziende più innovative e fra le stesse ed i rispettivi clienti o fornitori, il tutto acuito dallo sviluppo su scala globale dei rapporti lavorativi e commerciali[56].

Guardando adesso alle ricadute in termini giuridici dei processi appena descritti, esse concernono non solo la regolamentazione contrattuale attraverso la quale l'*outsourcing* prende vita ma anche una ulteriore serie di argomentazioni, comuni al *cloud*, delle quali ci si appresta a parlare nel prossimo capitolo.

[56] Cfr. A.MANTELERO, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali,* in Dir. Informatica, 4-5, 2010, pp. 673 e ss., in http://dejure.giuffre.it/psixshared/temporary/ftmp382940432.htm.

4. *La struttura del contratto di cloud*

Si consentita a questo punto - e in conclusione di questo secondo Capitolo - una disamina tecnica del contratto di *cloud*.

Strutturalmente, esso coinvolge e si articola essenzialmente sulla interrelazione tra tre soggetti:

. Il Fornitore di servizi - il c.d. c*loud provider* - ovvero colui che offre i servizi, quasi sempre secondo il già più volte richiamato modello *" pay-per-use";*

. il Cliente amministratore - ovvero colui che sceglie e configura i servizi offerti dal fornitore, generalmente garantendo al fruitore finale un valore aggiunto come ad esempio applicazioni *software*;

. Il Cliente finale - ovvero il fruitore ultimo dei servizi di *cloud*, colui che utilizza le risorse opportunamente configurati dal cliente amministratore.

Composti da tre distinti documenti, i contratti in esame[57] propendono, solitamente, per i due estremi: possono presentarsi particolarmente complessi o non esserlo affatto.

Innanzitutto è dato rinvenire le così dette *polices;* esse si materialmente, in due distinti fogli; uno nel quale si determinano gli aspetti inerenti al reciproco comportamento delle parti contrattuali, l'altro nel quale verranno stabilite le modalità di trattamento dei dati esportati nella nuvola[58].

Inerentemente ai contenuti, essi si concentrano essenzialmente intorno ai due poli focali appena richiamati, il primo inerente i profili generali del contratto, come ad esempio le condizioni generali alle

[57] La valutazione, comune in dottrina, deriva dall'analisi dei modelli contrattuali adottati, sino al gennaio del 2012 da quattro dei principali fornitori di servizi di cloud computing nonché detentori delle maggiori quote di mercato. Per una più estesa indagine, in questo caso su 27 fornitori, si veda l'indagine condotta nel 2010 dalla Queen Mary University of London, School of Law, in BRADSHAW-MILLARD- WALDEN, *Contracts of Clouds: Comparison and Analisys of the Terms and Conditions of Cloud Computing Services,* 1 september 2010, in http://ssrn.com.

[58] Tuttavia , in molti casi viene a mancare una coerente sistemazione della materia all'interno di questi documenti con la conseguenza che uno stesso aspetto può essere oggetto di disciplina congiuta, ma a volte anche disorganica e frazionata, in più di un documento. Cfr sul punto : A. MANTELERO, *Il contratto per l'erogazione alle imprese di servizi di cloud computing,* in Contratti e Impresa 4-5/2012, copia elettronica disponibile all'indirizzo :http://ssrn.com/abstract=2142050.

quali verrà offerto/erogato il servizio[59], l'altro attinente proprio alla gestione delle informazioni immesse *in the cloud*[60].

Se questa è la teoria, in pratica il rapporto contrattuale verrà quasi sempre improntato sullo schema, fin ora già richiamato in più di una occasione, " uno a molti" . Ciò vuol dire che quasi mai la contrattazione è personale e quasi sempre invece essa è standardizzata, con una definizione delle *policies* ad opera quasi esclusiva del fornitore ed una conseguente semplificazione estrema della fase precontrattuale, stante l'assenza pressoché assoluta della possibilità di variare o rinegoziare gli accordi.

Il ridotto potere contrattuale del cliente vuole anche dire impossibilità di adeguare il contratto alle esigenze nuove; la definizione di eventuali nuovi servizi ovvero l'offerta di nuovi prodotti, infatti, è sempre determinata solo ed esclusivamente ad opera del fornitore.

[59] E comprenderà determinazioni fondamentali, inerenti, tra l'altro, alla durata del vincolo contrattuale, alla lingua adoperata per la redazione dell'accordo, alla legge ed alla giurisdizione applicabili.

[60] Come ad esempio la gestione dei dati e dei flussi transfrontalieri, la loro sicurezza, le ipotesi di disclosure,.

Salvo per le ipotesi del così detto *lock-in,* ampia flessibilità è, invece, riscontrabile sotto il profilo della durata del vincolo contrattuale, quasi sempre rinegoziabile.

In conclusione sul punto, appare quindi evidente che la prassi contrattuale in via di formazione non è certo priva di criticità, anche assai rilevanti; vi è il problema della rigidità degli accordi sulla quale si è già detto, ma vi è anche una certa genericità, a volte assai pregnante, circa la natura e la tipologia delle prestazioni effettivamente oggetto del contratto con una conseguente difficoltà in ordine alla loro esatta individuazione, per non dimenticare poi la scarsa trasparenza di molte delle clausole inerenti questioni vitali quali le garanzie offerte o le ipotesi di esclusione della responsabilità. Considerato il fatto che i contratti aventi ad oggetto l'erogazione di servizi di *cloud* possono essere soggetti, anche più degli altri tipi di contratto, ad alterazioni funzionali significative quali l'inadempimento del fornitore dei servizi ovvero l'esecuzione negligente o in mala fede,

sono, secondo la dottrine[61], principalmente tre le aree principali cui dovrà porsi attenzione nell'esame di un contratto di servizi di *cloud*, ovvero innanzitutto i *Service Legal Agreement*, quindi il profilo della *privacy* e della riservatezza e sicurezza dei dati esportati in ambienti *cloud* oltre che, ovviamente le garanzie circa la conservazione e l'integrità dei dati stessi. Tralasciando al momento i due ultimi aspetti che verranno trattati innanzi, è opportuno in questa sede soffermarsi sul concetto e sul contenuto delle clausole costituenti i cosi detti SLA, ovvero i livelli minimi di servizio garantiti.

I *Service Level Agreement* costituiscono la parte forse più importante all'interno dei contratti di *cloud*; essi infatti tendono a definire con precisione l'oggetto del contratto e sovente riguarderanno parametri tecnici oggettivi e misurabili, importanti indicatori dell'effettivo livello qualitativo del servizio offerto[62]. È noto che in dottrina esiste una forte difformità di

[61] Cfr. G. RIZZO, *La responsabilità contrattuale nella gestione dei dati nel cloud computing*, relazione presentata al convegno "*Cloud Computing e Diritto – Questioni attuali e sfide future*", organizzato dall'Università Commerciale L. Bocconi, 17 maggio 2012.

[62] Ad esempio uptime e downtime, tempi di risposta, tempi di presa in carico del servizio, etc. Esiste allo stato una interessante attività di studio svolta da organizzazioni e consorzi industriali ed accademici finalizzata ad una sorta di "negoziazione intermedia" fra fornitori e utenti; un esempio è la SLA@SOI (http://sla-at-soi.eu/), un consorzio di ricerca finanziato dall'Unione Europea nell'ambito del VII

vedute circa l'inquadramento delle obbligazioni del *cloud service provider*: sono esse obbligazioni di mezzo o di risultato?

Nel dubbio si può comunque affermare che l'obbligazione *provider* sarà senza dubbio quella di eseguire le prestazioni pattuite in sede di SLA, e quindi nel puntuale rispetto dei livelli qualitativi di servizio prestabiliti, indipendentemente dalla qualificazione in termini giuridici della sua responsabilità. Tali livelli saranno generalmente riportati negli allegati tecnici al contratto o, nel caso di contratti elettronici, in documenti che siano espressamente richiamati nel contratto[63]; dalla combinazione, quindi, fra livelli di servizio promessi e regolamentazione della responsabilità per violazioni o incidenti discenderanno i primi fondamentali parametri per definire l'ambito della responsabilità del *cloud service provider* per inadempimento del proprio obbligo di fare. È stato correttamente osservato in dottrina che,

---

Programma Quadro. Fra i più recenti risultati di questi studi, cfr. WIEDER, BUTLER, *Theilmann and Yahyapour, Service Level Agreements for Cloud Computing*, Springer, 2011.

[63] Cfr. G. RIZZO, *op. cit.*.; A. ZINCONE, *Il contratto di outsourcing: natura, caratteristiche, effetti*, in Dir. aut., 2002, pag. 391.

anche nei rapporti *B2B*, molti fra i maggiori *cloud service provider* hanno di fatto imposto termini e

condizioni generali in base ai quali il servizio viene fornito *as it is*, *is*, senza alcuna garanzia di un determinato livello di *performance*. In tal caso, qualora il servizio divenisse indisponibile per un rilevante lasso di tempo l'utente non potrebbe dolersene né lamentare i conseguenti danni, sempre che l'inadempimento non dipenda da dolo o colpa grave.

Per tali ragioni è evidente che sono da preferire quei *provider* che rappresentino contrattualmente i livelli di servizio, previa una accurata valutazione da parte dell'utente della adeguatezza di tali *standard* di *performance* rispetto alle proprie esigenze professionali.

Normalmente, nei servizi commerciali che prevedono degli SLA precettivi, effettivi e non meramente indicativi, l'utente è indennizzato della indisponibilità del servizio mediante crediti sulla futura fatturazione ovvero attraverso una estensione della durata del servizio. E' questo un modo attraverso il quale il *provider* forfetizza il danno arrecato al cliente che, per parte sua, dovrà valutare previamente se il tipo di indennizzo offerto sia

sensato rispetto alla propria attività ed alle prevedibili ricadute negative, in termini di danni diretti ed indiretti, determinati dalla sospensione del servizio[64], oppure no.

Per concludere, la responsabilità per mancato raggiungimento degli *SLA* può rappresentare un terreno molto scivoloso; ciò perchè i *cloud provider* che si impegnano a mantenere un livello minimo di servizio[65] sovente prevedono, come rovescio della medaglia, una serie di eccezioni contrattuali, precipuamente delle esimenti da responsabilità, che finiscono col vanificare lo scopo funzionale e la stessa utilità dei *Service Legal Agreement* e delle garanzie che dalla

[64] Cfr. G. RIZZO, *La responsabilità contrattuale nella gestione dei dati nel cloud computing*, relazione presentata al convegno "*Cloud Computing e Diritto – Questioni attuali e sfide future*", organizzato dall'Università Commerciale L. Bocconi, 17 maggio 2012, il quale prosegue significativamente sul punto: "Nelle limitatissime ipotesi in cui l'utente avesse il peso negoziale per pretendere un contratto tailor made, è decisamente consigliabile porre particolare attenzione alla definizione degli SLA attraverso l'attenta predisposizione di allegati tecnici da accludere al contratto come parte integrante di esso. Oltre alla definizione dei SLA in via di allegato (questa tecnica redazionale si adatta particolarmente bene ai servizi di cloud computing vista la loro naturale scalabilità e la possibilità quindi per le parti di emendare un contratto modificando semplicemente un allegato tecnico) è consigliabile predisporre preventivamente una accurata ricognizione tecnica e gestionale dei bisogni del cliente ed una definizione puntuale dei criteri di monitoraggio e delle procedure di verifica dei livelli di servizio e delle prestazione [27], da trasfondere in altrettanti allegati tecnici. Si verrà quindi a formare un corpus di documenti tecnici che, una volta acclusi al contratto e resi parte integrante dello stesso, diverranno fondamentali per inquadrare ed interpretare esattamente le prestazioni dedotte in contratto e, conseguentemente, l'ambito di responsabilità del cloud service provider."

[65] Come spesso accade nei contratti IT, specie in quelli di outsourcing informatico.

loro predisposizione dovrebbero discendere. Per l'utente sarà quindi essenziale esaminare con attenzione l'estensione delle eventuali ipotesi di di irresponsabilità per valutare correttamente il rischio di eventuali inadempimenti.

CAPITOLO TERZO

CLOUD COMPUTING: LE PROBLEMATICHE

Sommario: *1. Le problematiche ricollegate al fenomeno del cloud: la questione della legge applicabile al contratto e del giudice competente; 1.2 I contratti B2B e l'abuso di dipendenza economica; – 2. La tutela della privacy dei dati; 2.2 Data retention, sicurezza ed integrità delle informazioni "in the cloud" – 3. Poteri e responsabilità dei soggetti coinvolti; 3.2 Violazione del contratto e risarcimento del danno; 3.3 Soluzioni assicurative contro i rischi derivanti dall'utilizzo dei servizi cloud – 4. Le nuove frontiere: il cloud e la Pubblica Amministrazione – Conclusioni.*

1. Le problematiche ricollegate al fenomeno del cloud: la questione della legge applicabile al contratto e del giudice competente

Nei capitoli precedenti si è tentato di delineare il fenomeno del *cloud computing*, attraverso l'analisi delle motivazioni sottese al suo utilizzo sempre crescente nonchè gli schemi contrattuali utilizzati per l'erogazione del servizio.

La tecnologia del *cloud computing*, riscuotendo un innegabile successo, è diventata, come si è più volte osservato, una realtà quotidiana, dall'uso domestico sino alle più avanzate applicazioni

in campo imprenditoriale; tuttavia, come per molte cose della vita, a tanti *pro* corrispondono altrettanti *contro*.

La " *nuvola* ", come sottolineato dalla quasi totalità degli studiosi del settore, è un fenomeno tendenzialmente transnazionale; ciò implica conseguentemente, un trasferimento transfrontaliero dei dati, che nel passaggio dal cliente al fornitore dei servizi, finiscono col travalicare quasi sempre i confini nazionali, in ragione del fatto che i *data center* di allocazione, o nel più dei casi i fornitori stessi, sono quasi sempre stranieri[66].

Queste circostanze spostano subito la nostra attenzione sui primi due problemi essenziali ai quali gli operatori del diritto sono invitati, a gran voce, a dare una soluzione: la legge applicabile al contratto e la determinazione della giurisdizione competente per le eventuali conseguenze che dalla sua esecuzione dovessero discendere.

La questione della legge applicabile è un aspetto destinato ad assumere grandissimo rilievo, soprattutto se si tiene conto che i servizi

[66] Spesso può capitare addirittura che, prima di giungere al gestore finale, i dati siano oggetto di trattamenti e trasferimenti intermedi.

offerti sono erogati, nella maggioranza dei casi, da prestatori localizzati non solo al di fuori dell'Italia ma addirittura dell'Unione Europea[67]ed in cui, in virtù del già menzionato rapporto uno a molti, i fornitori hanno interesse a gestire in maniera uniforme tali profili, ricorrendo, perciò, a clausole pattizie volte a definire in maniera generale e senza distinzioni la legge applicabile[68]. Consumatori, aziende e professionisti devono determinare con certezza la normativa cui fare riferimento in quanto il divario e la differenza di tutele che spesso s'incontra mettendo a confronto un ordinamento e un altro, soprattutto in materia di trattamento dei dati personali, potrebbe essere talmente elevate da rendere nulli, in caso di contenzioso, i benefici stessi ricollegati all'uso di sistemi di *cloud computing*[69]. Anzi condizione necessaria perché la crescita del

[67] I più risiedono negli Stati Uniti.

[68] Così A.MANTELERO, *Il contratto per l'erogazione dei servizi di cloud computing*, in Contratto e Impresa 4-5/2012 , pp. 1221 e ss. , il quale, incidentalmente, osserva che: "anche qualora venisse prescelta la legge italiana, potrebbero comunque emergere delle difficoltà interpretative, stante la predisposizione dei testi contrattuali sulla base di modelli statunitensi. In alcuni casi il ricorso ad istituti e concetti giuridici di *common law* può infatti risultare non agevolmente compatibile con la qualificazione degli stessi alla luce dell'ordinamento nazionale. Per una più ampia disamina di questi aspetti vedi G. DE NOVA, *Il contratto alieno*, Torino, 2010.

[69] Così E.BELISARIO, *"Cloud Computing", Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17*,* Altalex 2011, pag. 13 e ss.

mercato del *cloud* possa continuare indisturbata è proprio data dalla certezza in ordine alla normativa applicabile.

Ecco perché il tema della legge applicabile è un argomento di cruciale importanza ed è assai rilevante sotto molteplici aspetti; cosa succederebbe se ci fosse la rivendicazione della proprietà di un documento prodotto o memorizzato tramite un sistema di *cloud* ? Quali sarebbero le norme applicabili, quelle dello Stato che ospita il sistema di *cloud* o quelle dello Stato in cui il documento è stato prodotto? Ed ancora, quale garanzia avrebbero un'azienda, una Pubblica Amministrazione o un professionista nel caso in cui il contratto sia stato stipulato con una società con sede in uno stato diverso da quello in cui sono collocate le strutture informatiche?

La questione non è affatto di scarso rilievo ed è stata ed è fonte di ampio dibattito[70].

Come noto, vi è una grande differenza tra le norme applicabili nei Paesi facenti parte dell'Unione Europea e quelli extra-comunitari[71]; la

[70] E.BELISARIO, *op.cit.*

disciplina nazionale ed internazionale[72] non lascia spazio a dubbi interpretativi, prevedendo l'applicabilità al contratto della legge del Paese in cui il consumatore ha la residenza abituale. Pertanto, il quadro normativo da considerare sarà quello di almeno quattro distinti ordinamenti: quello del cliente, quello del fornitore del servizio *cloud*, quello del luogo in cui i dati sono stati allocati e memorizzati[73]e, in ultimo, ma non per importanza, quello del soggetto cui si riferiscono i dati trattati.

A questo punto, il conflitto di leggi applicabili che può venire a crearsi è facilmente intuibile.

Almeno limitatamente all'Unione Europea , il problema può incontrare una soluzione di pronto reperimento mediante l'applicazione della disciplina uniforme prevista per le obbligazioni

[71] Il gap e le differenze di tutela tra le norme applicabili nei Paesi facenti parte dell'Unione Europea e le leggi applicabili negli Stati Uniti d'America sono significative; tuttavia, ancor di più lo è il divario tra queste due realtà e i paesi terzi rispetto ad esse, in cui spesso, soprattutto per ragioni di carattere economico, sono ospitati i server dei cloud provider.

[72] Codice del Consumo, convenzioni internazionali, diritto internazionale privato e processuale.

[73] Spesso addirittura più di uno, nei casi della c.d. struttura multi-tenancy.

contrattuali ed extracontrattuali[74]. Ciò, tuttavia, per le sole ipotesi in cui la controversia sussista tra il cliente ed il fornitore, ovvero nei casi in cui la lite dovesse insorgere fra soggetti non legati da un vincolo contrattuale[75], rimanendo esclusi tutti gli altri casi. Si tratta però di una soluzione limitata nello spazio e perciò inadeguata; ciò in quanto l'orizzonte territoriale entro il quale il *cloud* viene adoperato - e perciò entro il quale possono aprirsi le controversi - è ben più ampio dei confini dell'Unione Europea, entro il solo perimetro della quale, purtroppo, è operante la normativa appena richiamata.

Vi è poi un altro problema: la determinazione della legge

applicabile dipende in concreto anche dalla materia oggetto di controversia[76]. A ciò si aggiunga che, su scala mondiale - lo scenario che, con buona pace di chi vorrebbe mettere limiti alla rete, deve essere

[74] Regolamento (CE) n. 593/2008 del Parlamento Europeo e del Consiglio del 17 giugno 2008 sulla legge applicabile alle obbligazioni contrattuali "Roma I", in G.U.C.E. n. L 177/6 del 04.07.2008 e Regolamento (CE) n.864/2007 del Parlamento Europeo e del Consiglio dell'11 luglio 2007 sulla legge applicabile alle obbligazioni extracontrattuali "Roma I", in G.U.C.E. n. L 199/40 del 31.07.2007.

[75] Come ad esempio nei casi in cui una persona fisica o giuridica lamentasse danni riconducibili ad una condotta di natura dolosa o colposa del cloud provider, esempio tipico la violazione della privacy, o anche del cliente del servizio cloud., anche se in questa seconda ipotesi è facile sussista un rapporto contrattuale fra il cliente cloud e il soggetto cui il dato si riferisce.

[76] Differendo a seconda che la controversia sia inerente la privacy, la responsabilità contrattuale o extracontrattuale, il diritto penale ovvero le investigazioni internazionali, il commercio elettronico, la proprietà intellettuale, ecc.

considerato quello proprio del *cloud computing*[77] - la materia diviene ancor più dinamica e complessa soprattutto in considerazione della diversità di approcci giuridici tra la nostra realtà e quella statunitense[78].

Si prenda, ad esempio, in considerazione l'ipotesi in cui si presentasse la necessità di un controllo dei dati a fini di indagini; la differenza di legislazione tra gli Stati, in tal caso, è particolarmente evidente. Si pensi alle sole differenze tra l'Unione Europea, dove il potere di ispezioni è relativamente limitato, e gli USA, dove la vigenza del *Patriot Act*[79] consente alle autorità di accedere, quasi

---

[77] Cfr. G. RIZZO, *La responsabilità contrattuale nella gestione dei dati nel cloud computing,* Relazione presentata al Convegno *" Cloud Computing e diritto – questioni attuali e sfide future"* organizzato dall'Università Commerciale L. Bocconi, Milano, 17.05.2012.

[78] Per un confronto fra i differenti approcci, calato nel contesto digitale, si veda A. MANTELERO, *Privacy digitale*, *in Manuale di informatica giuridica e diritto delle nuove tecnologie*, a cura di DURANTE e PAGALLO, Torino, 2012, pp. 159 e ss.. Con specifico riferimento al cloud computing C. HOOFNAGLE, Senior Fellow presso il Berkeley Center for Law & Technology, ha sottolineato che negli Stati Uniti il Quarto Emendamento alla Costituzione protegge senza dubbio i dati sui PC o i devices mobili in possesso dell'utente, ma quando, come nel cloud computing, i dati personali sono trasferiti a terzi la loro tutela diventa sensibilmente più affievolita , cfr. C. HOOFNAGLE*, Consumer Protection in Cloud Compunting Services*, Atti del convegno organizzato da Consumer Federation of America il 20-22 giugno 2010 alla New York University School of Law, successivamente pubblicato in Consumatori, Diritti e Mercato, 1/2011, pag. 92. Articolo disponibile anche su http://www.altroconsumo.it/nt/nc/news/cloud-computing-consumatori-diritti-e-mercato-16-n538300/download?ressourceUri=BFC2FB4EE5A5E2D9EC8106D7F3C122B8E669A2B6).

[79] Consultabile al seguente indirizzo: http://it.wikipedia.org/wiki/USA_PATRIOT_Act

senza limiti alle risorse dei *provider* e quindi eventualmente anche ai documenti e ai dati memorizzati su *server* di *cloud* residenti negli *States*.

Un ulteriore ambito in cui le norme variano in modo significativo è significativo è quello relativo al diritto d'autore ed all'attribuzione del del diritto di copia. Anche in tal caso l'uso del *cloud* potrebbe rivelarsi rivelarsi controproducente qualora si dovesse realizzare l'ipotesi in cui cui sia applicabile la legge di un Paese in cui tale diritto non sia tutelato; tutelato; in questo caso, è evidente che il soggetto che produca opere protette dal diritto d'autore potrebbe subire un grave pregiudizio[80].

Ed è qui che si acuisce l'importanza dello strumento

contrattuale; al fine di fornire quella certezza alle parti che già abbiamo visto essere indispensabile in un servizio come il *cloud* e che purtroppo non è dato trovare a pieno nella legge, si dovrà supplire proprio con il contratto; esso infatti rappresenta lo strumento principe mediante il quale le parti, *cloud provider* e cliente, regolano, nel metodo e nel merito, le questioni astrattamente suscettibili di sfociare in un

[80] Così E.BELISARIO, *"Cloud Computing", Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011, pag. 13 e ss.

conflitto, oltre, ovviamente, alle prestazioni oggetto del contratto ed alle modalità con cui devono essere rese.

Il contratto diventa quindi piattaforma di normalizzazione di una disciplina legislativa di certo incompleta - almeno se rapportata alla natura proteiforme del *cloud computing* ed alle innumerevoli implicazioni connesse al funzionamento dei servizi *cloud* - e di difficile coordinamento. Non solo: un chiaro e dettagliato accordo ha indubbie funzioni di trasparenza poiché , se ben redatto, ben negoziato e ben inteso dalle parti, consente all'utilizzatore del servizio di focalizzare l'attenzione sui vantaggi e sui rischi dello stesso, con esatta comprensione della qualità delle prestazioni promesse e delle garanzie relative ai dati trattati, utilizzati e immagazzinati presso i *data center* del *provider*, con una ulteriore prevenzione del rischio conflitti. Se, pertanto, in ragione della sua propria natura, la fruizione degli utilissimi servizi *cloud* comporta, come rovescio della medaglia, la perdita di controllo fisico dell'infrastruttura esportata sulla nuvola,

l'utente potrà comunque mantenere un certo controllo, seppur indiretto, sui propri dati, proprio grazie allo strumento contrattuale.

Se è vero, però, che prevenire è meglio che curare, e che un valido e dettagliato contratto pone parecchio al riparo da rischi, nel senso lato dell'espressione, è pur vero che tale tipo di presidio resta comunque meno efficace se la legge applicabile non è quella dell'utente, o, peggio, a quest'ultimo è addirittura sconosciuta e incomprensibile e se eventuali controversie dovranno essere composte da un giudice straniero, con un significativo aggravio, tra l'altro, dei costi[81].

Tutto ciò tenendo conto che la posizione di soccombenza resta sempre e comunque quella dell'utente; il *cloud provider* avrà infatti sempre l'interesse contrario dal momento che potrebbe rivelarsi antieconomico per lui confrontarsi con tanti ordinamenti giuridici quanti sono i clienti stranieri e tale circostanza è tanto più avvalorata se si tiene conto, ancora una volta, che i maggiori operatori del mercato *cloud* sono tutti soggetti che hanno la propria sede legale al di fuori dei confini dell'Unione Europea. Queste

[81] Si tenga conto poi, con specifico riferimento alla situazione italiana, che nel caso del cloud computing andrà anche valutata la possibilità di ottenere facilmente o meno l'esecuzione dei provvedimenti ottenuti dal giudice italiano, senza dover ricorrere a procedimenti complessi e onerosi.

considerazioni perciò, sottolineano quanto resta vivo - e da risolvere - il problema della individuazione di una disciplina normativa certa e comune, cui far soggiacere un negozio concluso tra soggetti situati fisicamente in stati diversi e ciò indipendentemente da un valevole strumento contrattuale.

Tecnicamente, e come già in precedenza accennato, secondo la disciplina generale il contratto si ritiene concluso nel luogo in cui si trova il proponente al momento dell'accettazione, ovvero nel luogo in cui l'accettazione giunge all'indirizzo del proponente; nell'ottica della soluzione al problema della uniformità di disciplina quindi, il primo riferimento normativo che potrebbe essere richiamato è dato dalla legge di riforma del diritto internazionale privato n. 218 del 1995, la quale, rinviando al regolamento CE n. 593/2008[82], riconosce efficacia generale alla Convenzione di Bruxelles in tema di competenza giurisdizionale nei contratti conclusi da consumatori.

Entrambi i dettati normativi dispongono che, nel caso di vendita di beni mobili materiali o di servizi, se vi è stata una forma di

[82] Sostitutivo della Convenzione di Roma del 1980.

pubblicità nel Paese del consumatore e questi ha compiuto nel proprio Paese gli atti necessari alla conclusione del contratto, si devono rispettare le norme imperative e la giurisdizione del Paese di residenza abituale del consumatore.

Ora, nel caso dei servizi di *cloud computing*, alla conoscenza degli stessi gli utenti arrivano spesso tramite siti internet; è perciò innegabile come tali siti realizzino una forma di comunicazione pubblicitaria anche assai pregnante. Pertanto, non si potranno eludere le norme imperative e di giurisdizione dello Stato di residenza del consumatore ogni qual volta il sito abbia avuto visibilità in tale ambito territoriale.

È, quindi, possibile, tra l'altro, affermare che lo *status* di consumatore è particolarmente importante ai fini della determinazione della legge applicabile.

Il legislatore italiano ha, altresì, escluso che, in caso di fornitore straniero, il consumatore possa essere privato della tutela minima richiesta dal Codice del Consumo, attraverso l'inserzione di clausole che prevedano

l'applicazione di una normativa straniera[83]. Perciò, quand'anche nel contratto ci fosse un esplicito riferimento all'applicazione di una legge straniera, il rinvio a detta legge non comporterebbe in modo alcuno il venir meno della tutela che il Codice del Consumo appresta al consumatore italiano.

Sempre all'interno di uno schema pattizio connotato dalla forza contrattuale del proponente l'accordo, sono frequenti, altresì, clausole volte a limitare la responsabilità del fornitore o le garanzie dallo stesso offerte in relazione alla prestazione erogata ovvero ancora derogatorie del foro competente.

Altro problema che si è posto in dottrina infatti - e che assume importanza sempre più rilevante nei contratti di *cloud computing* - è dato proprio dall'ipotesi in cui il fornitore straniero privi l'utente della tutela minima richiesta dal D.Lgs. n. 206/2005 attraverso l'inserzione nei suoi contratti - standardizzati - di clausole in cui esplicitamente si afferma che al rapporto contrattuale si applichi una normativa straniera. A tal proposito il legislatore, all'art. 143 del Codice del

[83] Art.143 Cod. Cons.

Consumo[84] è stato chiaro e molto rigido, introducendo una vera e propria clausola di garanzia in ordine a quella che deve essere la soglia minima di tutela che si ha l'obbligo di apprestare; va da se che tutte le clausole di segno opposto debbano considerarsi vessatorie e pertanto sottoposte al relativo regime giuridico, già in precedenza a grandi linee esaminato.

L'applicabilità del Codice del Consumo nel caso dei contratti di *cloud* appare particolarmente importante anche in considerazione degli specifici rimedi processuali previsti; si pensi, in particolar modo, all'azione di classe[85]. In dottrina si ritiene che, per le loro caratteristiche tipiche, i servizi di *cloud computing* potrebbero essere uno degli ambiti di applicazione dell'azione collettiva di cui all'art. 140-bis, D. Lgs. n. 206/2005 [86]forse più fortunati.

1.2 I contratti B2B e l'abuso di dipendenza economica

[84] "I diritti attribuiti al consumatore dal codice sono irrinunciabili. È nulla ogni pattuizione in contrasto con le disposizioni del codice. Ove le parti abbiano scelto di applicare al contratto una legislazione diversa da quella italiana, al consumatore devono comunque essere riconosciute le condizioni minime di tutela previste dal codice".

[85] La c.d. "*class action*".

[86] Si pensi, ad esempio, ad alcuni eventi come l'impossibilità temporanea di accedere alle risorse sulla nuvola oppure ad accidentali rivelazioni a terzi di dati o informazioni dell'utente; in questi casi, tutti i soggetti che si presumono danneggiati dalle condotte appena descritte potrebbero proficuamente utilizzare il rimedio della class action.

Occorre a questo punto un ulteriore distinguo tra i casi in cui il cliente sia un consumatore e quelli in cui invece ad accedere ai servizi di *cloud* sia un'impresa o un professionista.

Se è vero infatti che, come appena visto, nel caso di contratto concluso da un consumatore italiano o, quantomeno, europeo, godrà di una tutela minima ed inderogabile contro clausole inique ed irragionevoli, prestata in Italia dal Codice del Consumo e comunque garantita a livello europeo dalle direttive e dalle leggi nazionali di implementazione delle stesse[87], lo scenario cambia quando il negozio prenda corpo tra due soggetti di pari forza contrattuale ovvero nelle ipotesi di così detto rapporto *B2B*[88].

La relazione *B2B* è quella fra un fornitore di servizi di *cloud computing* ed un'impresa o un professionista: si tratta di categorie che, in quanto composte da soggetti privi della tutela minima di legge di cui al Codice del Consumo perchè non appartenenti alla categoria dei

[87] Che, a partire dalla fine degli anni ottanta, hanno progressivamente contribuito a dar forma al sostrato normativo del Codice stesso.

[88] Cfr. G. RIZZO, *La responsabilità contrattuale nella gestione dei dati nel cloud computing,* Relazione presentata al Convegno *" Cloud Computing e diritto – questioni attuali e sfide future"* organizzato dall'Università Commerciale L. Bocconi, Milano, 17.05.2012.

consumatori, risultano economicamente più esposte al rischio di eventuali *default* del *provider*[89]; esse dovranno perciò prestare maggiore attenzione al contratto ed, in particolare, alle condizioni che regolano la responsabilità del fornitore del servizio.

Gli operatori professionali quindi, pur se tipicamente destinatari di una protezione affievolita rispetto ai consumatori, non saranno in tal modo radicalmente privi di una tutela imperativa e successiva rispetto alla stipula di clausole particolarmente sbilanciate a favore di una delle parti.

Partendo ancora una volta dalla situazione di casa nostra, in Italia esiste la disciplina dell'abuso di dipendenza economica; a norma dell'art. 9 della l. 192/98, infatti, la legge definisce come dipendenza economica "la situazione in cui un'impresa sia in grado di determinare, nei rapporti commerciali con un'altra impresa, un eccessivo squilibrio di diritti ed obblighi".

[89] Si pensi ai profili di responsabilità nei confronti dei propri clienti.

Il divieto[90] colpisce, sanzionandole con la nullità, salvo il diritto al risarcimento del danno della parte che ha subito l'abuso, tutte le ingiustificatamente gravose cui è sottoposta un'impresa , cliente o fornitrice, che si trova in uno stato di dipendenza economica rispetto impresa committente, la quale ultima è nella concreta facoltà di imporre al partner condizioni eccessivamente squilibrate a proprio vantaggio[91].

La dipendenza economica deve essere valutata " tenendo conto anche della reale possibilità per la parte che ha subito l'abuso, di

reperire sul mercato alternative soddisfacenti[92]": è questo il criterio essenziale di riferimento nell'applicazione della norma, che

[90] Originariamente elaborato in materia di subfornitura e poi esteso per giurisprudenza costante a tutti i contratti di cooperazione commerciale

[91] La legge parla di "eccessivo squilibrio di diritti ed obblighi", locuzione che riecheggia il "significativo squilibrio di diritti ed obblighi" in tema di clausole abusive. La dottrina ha tuttavia chiarito che le due formulazioni non sono conciliabili ai fini di una interpretazione sistematica: in questo senso V. PINTO, *L'abuso di dipendenza economica «fuori dal contratto» tra diritto civile e diritto antitrust*, in Riv. dir. civ., 2000 pag. 394; G. COLANGELO, *L'abuso di dipendenza economica tra disciplina della concorrenza e diritto dei contratti – Un'analisi economica e comparata*, Torino, 2004, pag. 79; S. BENUCCI, *Le prime pronunce in tema di «abuso di dipendenza economica»,* in VETTORI (a cura di), Concorrenza e Mercato, pag. 485; contra F. PROSPERI, *Il contratto di subfornitura e l'abuso di dipendenza economica*. *Profili ricostruttivi e sistematici*, Napoli, 2002, pag. 297.

[92] G. OPPO, *Princìpi*, Torino, 2001, pag. 43; sul punto anche A. MAZZIOTTI DI CELSO, *Abuso di dipendenza economica,* IN G. ALPA – A. CLARIZIA (a cura di), *La Subfornitura, Commento alla legge 18 giugno 1998, n. 192*, Milano, 1999, pag. 247. Secondo V. PINTO, op. cit., pag. 405 quello della reale

crea un addentellato alle concrete dinamiche di mercato[93]. L'ambito di tutela destinato agli utenti professionali non è limitato al solo ambito nazionale; sebbene l'art. 9 della legge 192/98 non abbia una diretta e chiara matrice comunitaria esso è evidente espressione della disciplina europea in materia di libera concorrenza nel mercato. Inoltre la fattispecie non è affatto estranea alla legge ed alla giurisprudenza di molti altri Stati membri dell'Unione, come ad esempio la Francia e la Germania[94]. Nel sistema giuridico britannico poi, le piccole e medie imprese non sono prive di una tutela contro condizioni inique e dall'analisi casistica emergono esempi assolutamente calzanti rispetto all'ipotesi di relazioni contrattuali aventi ad oggetto servizi di *cloud computing*[95] .

---

sostituibilità sarebbe l'unico criterio legale di accertamento dell'abuso di dipendenza economica fermo restando che nel concreto atteggiarsi dei rapporti se ne potrebbero riscontrare altri. Cfr. altresì, per tutti, G. RIZZO, *La responsabilità contrattuale nella gestione dei dati nel cloud computing,* Relazione presentata al Convegno *" Cloud Computing e diritto – questioni attuali e sfide future"* organizzato dall'Università Commerciale L. Bocconi, Milano, 17.05.2012.

[93] Cfr. G. RIZZO, *Op.Cit.*

[94] Nella relazione di accompagnamento alla legge 192/1998 si evidenziava chiaramente che l'art. 9 trova quale «referente comparatistico [...] il paragrafo 26, comma 2, secondo periodo [ora § 20, comma 2], della normativa antimonopolistica tedesca (GWB), ripresa dal legislatore francese nell'art.8, lettera b), dell'ordinanza 1° dicembre 1986, n.1243 [ora art. L. 420 – 2 del Code de commerce]».

[95] Cfr. G. RIZZO, Op. Cit.; Si rammenta in proposito che nel caso Kingsway Hall Hotel v. Red Sky IT (Houslow) [2010] EWHC 965 (TCC). In tale precedente è emerso il principio di diritto secondo cui in un contratto per servizi IT concluso fra un imprenditore non specialista del settore ed un imprenditore specialista determinate clausole, sebbene racchiuse in condizioni generali di contratto, possono

Inoltre, con prospettiva ancor più ampia, principi analoghi a quelli appena rammentati sembrano contenuti nella nuova *lex mercatoria,* nei "*Principles of International Commercial Contracts*" [96]*Unidroit*, nel quadro dei quali la disciplina sul contraente debole trova espressione nell'istituto della *Gross Disparity* .[97]

Queste osservazioni assumono significato ancor più importante se si tiene conto che l'abuso tende ad assumere rilevanza non solo e non tanto al momento della conclusione del contratto quanto nell'intero

considerarsi inique e sleali (unfair) e non efficaci (unenforceable). Sebbene il caso concreto non riguardasse servizi cloud applicabile alla verifica dei contratti di cloud computing. Il precedente è riportato in BRADSHAW, MILLAR E WALDEN, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 63/2010, pag. 16 e ss. Disponibile su http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374 e successivamente pubblicato, con alcuni aggiornamenti, in International Journal of Law and Information Technology, 2011, 19 (3), pagg. 187-223.il ragionamento della corte, appuntandosi sulla elevata specificità di determinate condizioni contrattuali e sulla asimmetria conoscitiva delle parti, è assolutamente

[96] Cfr. G. RIZZO, *Op.Cit.*. Tali principi – come noto – dettano specifiche regole (ancorché di soft law) in tema di conclusione del contratto, vizi del volere, invalidità, interpretazione, contenuto del contratto, adempimento, sopravvenienze, inadempimento, e risoluzione, e la cui essenza è stata proprio rinvenuta nell'opera di coordinamento delle pratiche internazionali con i principi generali del diritto universalmente accolti, così da contemperare le caratteristiche proprie della lex mercatoria quale diritto unilateralmente creato dalla classe imprenditoriale con le esigenze di protezione del contraente debole.

[97] Art. 3.10.; Tale disposizione consente, infatti, di chiedere l'annullamento o la modifica del contratto o di una singola clausola che attribuisca ad una parte un vantaggio eccessivo qualora detto vantaggio appaia ingiustificato in base ad una serie di fattori di natura soggettiva (imperizia, ignoranza, inesperienza o mancanza di abilità a trattare) ed oggettiva (natura e scopo del contratto). I presupposti per agire in base a tale disposizione sono, pertanto, rappresentati da un lato dal vantaggio eccessivo a favore di una parte, che secondo il commento ufficiale, si ha quando vi sia una ragguardevole disparità di valore tra le prestazioni tanto che un tale squilibrio sia "so great as to shock the coscience of a reasonable person", e dall'altro dalla mancanza di giustificazione di tale vantaggio.

corso della sua esecuzione o addirittura al momento della cessazione, del rapporto se non anche oltre, per via delle significative conseguenze che ne derivano. La casistica giurisprudenziale non contempla evidentemente ancora contenziosi su servizi di *cloud computing*, ma per quanto detto sinora è indubbio che la norma potrebbe trovare applicazione ad ipotesi in cui dovesse verificarsi un *lock in* assoluto o relativo[98] a sfavore dell'utente.

2. La tutela della privacy dei dati

Come già osservato, il *cloud computing* comporta necessariamente il trasferimento dei dati e, in molti casi, genera addirittura flussi e circolazione transfrontaliera degli stessi.

Ecco quindi che, proprio per questo motivo, altro rilevante problema posto dalla diffusione dei sistemi di *cloud computing* risulta proprio essere quello relativo alla riservatezza dei dati che l'utente immette "*in the cloud*".

[98] Il lock in assoluto è il caso di impossibilità tecnica assoluta o relativa per l'utente di esportare i dati immagazzinati presso il cloud provider in un formato idoneo a permetterne il caricamento in propri server o presso altri cloud provider. Per lock in "relativo", invece, si vuol indicare il caso in cui il cambio di fornitore implichi dei costi rilevanti per il cliente. Cfr. G. Rizzo, *La responsabilità contrattuale nella gestione dei dati nel cloud computing,* Relazione presentata al Convegno *" Cloud Computing e diritto – questioni attuali e sfide future"* organizzato dall'Università Commerciale L. Bocconi, Milano, 17.05.2012.

Quello relativo alla protezione dei dati personali, alla loro sicurezza ed alla loro riservatezza, rappresenta uno dei fattori di maggiore criticità nello sviluppo dei servizi *cloud*[99] ed una delle maggiori preoccupazioni per gli utilizzatori del servizio; allo stato, gli utenti, infatti, sono attratti dai vantaggi della nuvola ma, al tempo stesso, sono frenati dal timore di perdere il controllo dei propri documenti e delle proprie informazioni[100]. A ciò deve aggiungersi che la gran parte degli utenti di internet ha sperimentato servizi di *cloud computing* senza rendendosene conto e senza nemmeno conoscere la tecnologia che li rende possibili[101]. Ciò perché molto spesso, e soprattutto nelle ipotesi di *Public Cloud*, l'utilizzo dei servizi di *cloud computing* non è collegato alla sottoscrizione di un accordo contrattuale in senso tecnico, bensì alla mera "registrazione" *on-line*

[99] Sui profili legati alla riservatezza dei dati personali nell'ambito del cloud computing, va richiamato, ancora una volta, l'interessante contributo di A. MANTELERO , *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, in Dir. Inf., 2010, 673 ss.. L'Autore individua nel *SaaS* tre diverse fasi di trattamento: immissione dei dati avvalendosi dell'interfaccia software, elaborazione degli stessi ad opera del software, gestione dei dati elaborati (archiviazione, copiatura, back up, invio a terzi, ecc).

[100] Drastica, al riguardo, l'autorevole voce di Richard Stallman , fondatore della Free Software Foundation, che ha affermato testualmente: " il cloud computing è pericoloso ed è stupido utilizzarlo" ; cfr. http://news.cnet.com/8301-1001_3-10054253-92.html.

[101] Così E.BELISARIO, *"Cloud Computing" , Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011, pag. 13 e ss.

che consente di accedere al servizio senza che questi abbia una effettiva conoscenza del fenomeno di esternalizzazione sotteso alla immissione dei dati nella *cloud*. Tale mancanza di consapevolezza è tanto più grave se si considera che essa è, spesso, conseguenza della prassi per cui nei contratti di servizio o nei termini e condizioni d'uso, i *providers* non fanno specifico riferimento al fatto che i servizi sono erogati in base ad un sistema di *cloud computing*.

Ancora, come già visto, i dati importati "*in the cloud*" non risiedono in maniera permanente sul medesimo *server* bensì vengono continuamente spostati da una luogo all'altro in ragione della loro allocazione ottimale; questo processo incide ulteriormente sul loro trattamento in termini di tutela della *privacy*.

Da queste considerazioni, è agevolmente comprensibile che assume rilevanza conoscere dove, in che modo ed a quali condizioni viene offerta la gestione dei dati; il *cloud provider,* infatti, deve gestire anche il complesso degli aspetti relativi alla sicurezza rispetto all'accesso di terzi non

autorizzati ai dati, alla possibilità di distruzione o perdita dei dati medesimi, alla loro alterazione nonché alla loro sottrazione.

ll *cloud computing* è, nelle più recenti analisi, considerato un tema prioritario non solo dell'agenda dei privati quanto soprattutto di molte imprese. Il processo di esternalizzazione di attività e per essa, di massicci blocchi di dati di ogni sorta, giunge con il *cloud* alla sua fase più estrema; saranno, infatti, le banche dati aziendali ma anche private, a poter lasciare i locali dell'impresa o del pc della propria casa per essere ospitate presso reti di *data center* gestite da soggetti terzi.

Il rischio di perdere il potere di controllo sui dati è, come già in precedenza accennato, ovviamente altissimo anzi inevitabile, quantomeno parzialmente, con tutti i rischi collegati, in particolare ove la infrastruttura *cloud* venga utilizzata anche per la conservazione di informazioni aziendali strategiche o, comunque, di natura confidenziale. È bene, quindi, che chi sceglie l'utilizzo dei servizi di *cloud* sia consapevole, per un verso, dei rischi che si assume e, per l'altro delle possibili responsabilità alle quali si espone nei confronti di

terzi come clienti, fornitori, dipendenti, per eventuali violazioni della normativa in materia di *privacy*.

La domanda apicale resta perciò come tutelare i cliente nei confronti del fornitore e quali siano le responsabilità nei confronti dei terzi i cui dati personali sono stati violati.

Il tema, ancora una volta, va affrontato in una prospettiva internazionale, in considerazione del fatto che il mercato del *cloud* è affollato da *players* globali e la nuvola può essere costituita, come già evidenziato, da reti di *data center* localizzati in svariati Paesi europei ed extraeuropei. Il primo problema sarà, dunque, ancora lo stesso: capire quale legge regoli i rapporti con il *provider* sotto il profilo della tutela dei dati personali e quale giudice potrebbe essere adito qualora fossero state riscontrate delle inadempienze da parte del fornitore. È un dato notorio che il quadro normativo europeo in materia di protezione dei dati personali, fondato sulla Direttiva 95/46/CE, offre tutele giuridiche in materia di *privacy* che i Paesi extra UE - Stati Uniti compresi - in molti casi non sono in grado di assicurare.

La disciplina comunitaria è particolarmente restrittiva rispetto al flusso transfrontaliero di dati, fenomeno[102] che nel settore in commento rappresenta praticamente la regola. Il trasferimento dei dati verso un Paese extra UE è infatti possibile solo "se il paese terzo di cui trattasi garantisce un livello di protezione adeguato". Ad oggi sono molto pochi i Paesi inclusi in tale novero: Svizzera, Ungheria, Canada, Argentina, Baliato di Jersey, Isola di Man, Isole Faroer, Principato di Andorra, e Stato di Israele.

Ma vi è di più. Anche in ambito europeo, seppur in presenza di un nucleo centrale di principi condivisi, la normativa di dettaglio varia da Paese a Paese in base al maggiore o minore rigore adottato da ciascuno Stato in sede di recepimento della direttiva comunitaria, così come variano i relativi adempimenti a cui è tenuto il titolare al fine garantire una piena *compliance* al trattamento di dati personali posto in essere. La Francia non consente, ad esempio, in assenza di una specifica

[102] L'invio dei dati in Paesi in cui il livello di protezione è più basso di quello sancito dalla disciplina comunitaria è "potenzialmente rischioso per la tenuta dell'intero sistema delle garanzie definite in materia" ; così A. MANTELERO, *Processi di outsourcing,* cit., pag. 688. Per comprendere come mai il rischio non riguardi solo il trasferimento verso i Paesi meno sviluppati o con un deficit di democrazia, si veda il confronto fra modello europeo e nordamericano in A. MANTELERO, *Privacy digitale*, pagg. 162 e ss.

autorizzazione amministrativa, il trasferimento di dati sensibili[103] al di fuori dei confini nazionali; differenti sono, poi, le regole adottate da ciascun Paese europeo in materia di *data retention*, con la previsione di diversi tempi massimi di conservazione dei dati.

La Direttiva 95/46/CE ha trovato applicazione in Italia attraverso il nostro Codice della *Privacy*, introdotto col Decreto Legislativo n.196 del 30 giugno 2003. Secondo la normativa ivi prevista, l'individuazione della legge applicabile viene determinata in base a criteri essenzialmente territoriali[104]

---

[103] Ad esempio, i dati relativi alla salute.

[104] E'opportuno ricordare come il D.Lgs. n. 196/2003, riprendendo la normativa comunitaria n. 95/47/CE, distingua tra trasferimento dei dati all'interno dell'Unione Europea e trasferimento dei dati verso paesi terzi. Per quanto concerne la prima ipotesi non sono previste particolari restrizioni dal momento che tutte le legislazioni nazionali sono state adeguate ai principi enunciate dalle direttive comunitarie; l'art. 42 Codice Privacy prevede infatti che "*le disposizioni del presente codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni*". Al contrario, come facilmente intuibile, sono molto più problematici i trasferimenti verso Paesi che non siano membri dell'Unione Europea in quanto tali Paesi - di norma - non hanno normative di tutela di riservatezza dei dati personali simili a quella comunitaria. L'art. 43 D.Lgs. n. 196/2003, inoltre, prevede che il trasferimento di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione Europea è comunque consentito quando: l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta; è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato; è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21 del medesimo Codice; è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità

che, effettivamente, mal si conciliano con la nuvola; essi sono il principio dello stabilimento del titolare, ovvero l'utilizzo di strumenti e strutture presenti sul territorio europeo. Tali disposizioni implicano delle conseguenze chiarissime: il semplice spostamento della sede della società e dei *data center* al di fuori del territorio europeo potrebbe consentire al *provider* di sottrarsi ai vincoli previsti in materia

---

fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato; è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale; è effettuata una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia; è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A) D.Lgs. n. 196/2003, per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi della normativa vigente in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati; il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni. Di conseguenza, i soggetti tenuti all'applicazione del D.Lgs. n. 196/2003 dovranno necessariamente acquisire preventivamente dal fornitore di servizi *cloud* l'informazione relativa al luogo in cui verranno trattati i dati; a tal proposito l'art. 44 Codice Privacy prevede anche che - fuori dalle ipotesi precedentemente enunciate - il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato individuate: dal Garante anche in relazione a garanzie prestate con un contratto o mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo. In questo caso, l'interessato può far valere i propri diritti nel territorio dello Stato, in base al presente codice, anche in ordine all'inosservanza delle garanzie medesime; con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

di *privacy* dalla normativa comunitaria, anche laddove i propri servizi fossero diretti principalmente al mercato europeo**.** In tali circostanze, appare auspicabile una accorta selezione del *provider,* anche attraverso una chiara mappatura della rete di *data center* ove i dati della società potrebbero essere ospitati. La normativa europea e quella italiana vietano, infatti, il trasferimento di dati personali verso Paesi extra Ue che non assicurino un adeguato livello di protezione, salvo che, prima di procedere al trasferimento, non vengano adottate adeguate salvaguardie, anche di natura contrattuale, per la protezione dei dati personali. Per il caso in cui l'infrastruttura del *provider* sia costituita da una rete di *data center* localizzati in diversi Paesi extra Ue, al fine di non esporsi a possibili rischi legali nei confronti proprio, dei propri clienti, dipendenti e fornitori se trattasi di azienda o, quantomeno, per contenerli il più possibile, il privato o la società cliente, prima di inviare i dati, personali o dei propri clienti, dovrebbe assicurarsi che il trasferimento degli stessi sulla nuvola e quindi da Paese a Paese avvenga sempre nel rispetto di quelle garanzie minime di sicurezza previste dalla legge europea. Peraltro, tra gli strumenti negoziali

approvati dalla Unione Europea, l'adozione del set di clausole contrattuali standard per il trasferimento di dati da un titolare Ue ad un responsabile extra Ue, sembra essere il solo ad adattarsi alle specifiche esigenze del *cloud*. Gli strumenti negoziali alternativi appaiono, infatti, difficilmente adattabili al *cloud*: le *Binding Corporate Rules*[105] non sono suscettibili di applicazione per i trasferimenti all'esterno di un medesimo gruppo societario ed i principi del *Safe Harbor*[106] non sono estensibili ad altri Pesi extra Ue. Peraltro, l'Autorità Garante tedesca - con una pronuncia del 18 giugno 2010 - si è espressa nel senso di ritenere i principi sanciti dal *Safe Harbor* non idonei ad offrire adeguate garanzie di protezione dei dati nel contesto dei servizi *cloud*. Anche sotto questo profilo, indispensabile appare una accurata mappatura della rete di *data center* ove i dati trasferiti potrebbero essere ospitati. La trasparenza della piattaforma del fornitore è estremamente rilevante anche per una ulteriore ragione: la presenza fisica dei *server* in uno Stato comporterà per l'Autorità Giudiziaria di

[105] Ovvero le regole per i trasferimenti internazionali di dati infragruppo.
[106] Il protocollo che regola i trasferimenti di dati verso gli Stati Uniti .

quello Stato la possibilità di dare esecuzione ad ordini di esibizione, di accesso o di sequestro, ove sussistano i presupposti giuridici in base alle alle leggi di quel Paese. Per converso, rispetto a quei medesimi *data base*, l'Autorità Giudiziaria italiana potrà conseguire i medesimi risultati solo a mezzo di complicate rogatorie internazionali. Non è, quindi, indifferente per una società, un privato o un ente pubblico sapere che i propri dati si trovino in un *server* in Italia, in Europa o in un imprecisato Paese extraeuropeo[107]. Al fine di contenere i possibili rischi, appare, dunque, imprescindibile un'accorta individuazione dell'operatore al quale i propri dati saranno affidati, anche attraverso una valutazione di parametri "collaterali" quali la solidità finanziaria e il grado di trasparenza e di sicurezza garantito dalle *policy* aziendali del *partner* prescelto. Ancora una volta fondamentale sarà la scelta di adeguati strumenti negoziali che assicurino capienti e

[107] Non a caso Francesco Pizzetti, ex presidente dell'Autorità Garante per la Privacy, nella sua ultima relazione annuale ha posto l'attenzione proprio sul tema del cloud computing, osservando che: " Occorre riflettere anche sui rischi che pone la nuova tecnologia del "cloud computing", con la quale i dati verranno sempre più sottratti alla disponibilità materiale di chi li produce e usa, e gestiti da enormi server collocati in ogni parte del pianeta. Un fenomeno che moltiplicherà i servizi di "remote hard disk" e renderà sempre più ampio il ricorso all'outsourcing e all'hosting dei sistemi, moltiplicando i servizi forniti da terzi secondo modalità che favoriscono sempre di più la delocalizzazione dei dati conservati. Si tratta di una nuova frontiera che allarma tanto le strutture militari quanto quelle di sicurezza interna, e che coinvolge problemi di enorme portata."

significative garanzie nonché obblighi di notificazione per il caso di perdita o di accesso non autorizzato ai dati affidati in custodia. Come già accennato, è importante inoltre che nel contratto siano contenuti precisi parametri che, attraverso la definizione di livelli di servizio minimi qualitativi e quantitativi - i già richiamati *Service Level Agreements* - permettano di misurare le prestazioni del fornitore e le misure di sicurezza garantite. Così come saranno opportune - onde scongiurare i già più volte menzionati rischi di *lock in* - clausole che disciplinino i tempi e le modalità di transizione dei *data base* da un fornitore ad un altro, nel caso di risoluzione o cessazione del contratto, con una precisa individuazione delle obbligazioni gravanti sul fornitore al termine del rapporto.

Riassumendo, alla luce di tale assetto, che dovrebbe essere quello di maggiore garanzia per l'utente laddove veramente dovesse realizzarsi, dovranno essere considerati due aspetti: nel caso di rapporto titolare-responsabile, l'utente dovrà[108] principalmente assicurarsi di avere un controllo effettivo sui dati; selezionare un

[108] Cfr.: art. 17, dir. 95/46/CE

responsabile del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare; assicurarsi del rispetto di tali misure. Se il rapporto fra utente e *cloud provider* si delinea invece come fra due titolari autonomi o fra contitolari, il problema più rilevante è quello del trasferimento all'estero dei dati personali[109]. Nell'ipotesi più frequente, quindi, l'utente dovrà principalmente accertarsi di essere nelle condizioni di esercitare un effettivo controllo sui dati comunicati al *cloud provider* ai fini del rispetto delle misure di sicurezza imposte al *provider*[110]. È intuibile come si tratti di un'impresa alquanto ardua, soprattutto in considerazione del normale

[109] Per un inquadramento delle implicazioni del trasferimento dei dati all'estero, cfr. G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pagg. 282 e ss.

[110] Sarebbe utile che l'utente svolgesse una verifica preventiva al fine di valutare che gli standard di sicurezza del provider siano ragionevoli o comunque commisurati alla rilevanza dei dati affidatigli. Naturalmente le forme di questa verifica potranno essere le più varie: dal semplice studio ed approfondimento e comparazione delle offerte tecniche dei vari provider ad una interazione vera e propria, ove concretamente possibile, con questi ultimi (esplicite richieste di informazioni, questionari, incontri fra i rispettivi tecnici, ecc.), tutto al fine di chiarire i profili di gestione dei dati nel sistema del cloud provider e garantire nei limiti del possibile all'utente un adeguato grado di controllo sul flusso dei dati. Un importantissimo elemento da considerare nella verifica preliminare del fornitore del servizio cloud è poi il rispetto, da parte di quest'ultimo, di idonei standard specificamente relativi alla gestione della sicurezza delle informazioni, in particolare i c.d. ISO/IEC 27001, certificabile da organismi terzi e quindi effettivamente verificabile dall'utente e ISO/IEC 27002, complementare al primo soprattutto nell'ottica dell'implementazione dei controlli, ma non certificabile da organismi terzi.

sbilanciamento fra i poteri negoziali delle parti, delle asimmetrie informative esistenti e, non ultimo, della impossibilità talvolta per lo provider di indicare con sicurezza dove i dati esattamente risiedano[111].

Nei tempi più recenti, la disciplina europea sulla *privacy* e il suo incisivo condizionamento in positivo in ordine alle scelte degli utenti il *cloud provider* cui affidarsi, ha spinto molti dei maggiori operatori a dotarsi di *data center* siti in Paesi europei e ciò al fine di agevolare la propria penetrazione commerciale nel mercato europeo. Se questo alcuni dei problemi sopra evidenziati, ne fa sorgere di nuovi e più complessi tutte le volte in cui il *cloud provider* stabilito nell'Unione Europea si avvalga di soggetti terzi extra UE in qualità di subincaricati del trattamento dei dati. Mancano in questo caso delle clausole tipo approvate dalla Commissione[112]. Sono state

[111] Questo a causa dalla infrastruttura molto spesso assai complessa del provider e dalle stesse procedure di gestione dei dati implementate da quest'ultimo al fine di garantire funzionalità come back-up, scalabilità, ecc.

[112] Interessante al riguardo quanto osservato dal Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali, Parere 3/2009 sulla proposta di decisione della Commissione relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi, a norma della direttiva 95/46/CE, Bruxelles, 5 marzo 2009.

quindi ventilate alcune soluzioni, fra le quali un rapporto contrattuale diretto fra il titolare europeo ed il subincaricato non europeo che preveda l'inclusione delle clausole tipo di cui alla decisione 2010/87/CE[113], un chiaro mandato all'incaricato europeo di usare le clausole di cui alla decisione 2010/87/CE nel suo rapporto contrattuale

con il subincaricato non europeo; contratti *ad hoc*, previa approvazione delle competenti autorità del Paese dell'esportatore.

2.2 Data retention, sicurezza ed integrità delle informazioni sul cloud

Dalla lettura del quadro normativo appena ricostruito, con tutte le incongruenze che purtroppo lo caratterizzano, è chiaro che l'utente dei servizi *cloud* non potrà non prestare attenzione, nella scelta del suo fornitore, alla collocazione geografica dei *server* da quest'ultimo utilizzati; i moduli contrattuali impiegati dovranno, pertanto, contenere clausole che chiaramente predispongano e disciplinino l'eventuale trasferimento, anche transfrontaliero, dei dati immessi nella nuvola. Ma oltre che sotto il profilo della riservatezza dei dati, la collocazione geografica dei *data center* sarà rilevante anche sotto altri profili. Il *cloud computing* pone un ulteriore

[113] In questo caso il subincaricato viene trattato alla stregua dell'incaricato principale.

problema in relazione alle norme che disciplinano la conservazione dei dati per la repressione delle attività criminose. Anche questo è un aspetto che rientra nel più vasto concetto di conservazione dei dati anche se non propriamente legato alla loro sicurezza ed alle responsabilità dell'utilizzatore della nuvola. Tuttavia è possibile considerarlo come un altro tema delicato in relazione ai tempi ed alle modalità di mantenimento in vita dei dati stessi, questa volta per ragioni legate alle indagini giudiziarie[114]. Si pensi al fenomeno della *data retention*, ossia la raccolta automatizzata dei dati degli utenti al fine di supportare gli organi d'indagine in caso di eventuali investigazioni. Ciò a seguito della crescita esponenziale della commissione di reati proprio attraverso l'utilizzo delle più moderne tecnologie ed alla necessità di conservare evidenze che consentano un più agevole perseguimento delle condotte antigiuridiche; per questo le legislazioni di numerosi Paesi hanno investito alcuni soggetti privati, come i fornitori di servizi di comunicazione elettronica, dell'obbligo di

[114] Cfr. E.BELISARIO , *" Cloud Computing" , Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011 pp. 22 e ss

raccogliere e conservare per un determinato periodo di tempo alcuni dati personali relativi agli utenti. In quest'ipotesi, il *provider* è per legge onerato della responsabilità relativa alla conservazione dei dati che potrebbero essere richiesti all'Autorità competente nell'ambito dell'attività di indagine.

A livello comunitario, pur con le dovute differenze tra le diverse legislazioni, si è affermato il principio per cui vanno contemperati i contrapposti interessi tra la sicurezza degli individui, vero obiettivo delle norme in materia di *data retention*, e quello di garantire la riservatezza degli utenti che sarebbe compromesso oltremisura nel caso in cui i dati venissero conservati per tempi più lunghi di quelli effettivamente necessari per eventuali indagini[115]. In materia, la normativa di riferimento è la Direttiva 2006/24/CE che disciplina i tempi di conservazione delle informazioni e dei dati degli utenti per un periodo compreso tra i 6 e i 24 mesi.

In Italia la *data retention* è regolata nel Titolo X del Codice *Privacy*, così come modificato dal D.Lgs. n. 109/2008[116].

---

[115] Cfr.: E. BELISARIO, *Op.Cit.*

[116] In particolare l'art. 122 D.Lgs. n. 196/2003 prevede che "è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente"; conseguentemente, è previsto (art.

Un'altra area critica inerentemente ai servizi di *cloud* risulta dunque essere quella della integrità e sicurezza dei dati dell'utente, questa volta però non nell'ottica del rispetto delle norme di ordine pubblico a tutela della *privacy* quanto piuttosto del diritto - anche patrimoniale, soprattutto quando trattasi di dati aziendali - dell'utente stesso a mantenere il controllo, la disponibilità e la segretezza di tali informazioni.

123) che i dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica. Tuttavia, in via del tutto eccezionale e per finalità di sicurezza pubblica, accertamento e repressione dei reati, è previsto dall'art. 132 che "i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione"

3. Poteri e responsabilità dei soggetti coinvolti

Necessaria è, a questo punto, una riflessione sulla definizione dei poteri e delle responsabilità dei soggetti coinvolti nell'erogazione e nell'utilizzo dei servizi di *cloud computing*. La struttura della nuvola sembra, infatti, scardinare le categorie tradizionali così come disciplinate dal Codice della *Privacy*, divise nella dicotomia titolare-responsabile del trattamento dei dati personali[117] in favore di una costruzione anomala dei ruoli, dove il fornitore dei servizi di *cloud computing* appare più che altro come una figura ibrida; non è, infatti, il titolare del trattamento dei dati, ma più che altro una sorta di mero custode delle banche dati del cliente, anche se, ad un'attenta analisi, anche questa definizione non risulterà delle più appropriate per descrivere il suo ruolo.

Preliminare allora sarà l'esame dei profili di responsabilità e la disamina dei ruoli e degli attori che possono intervenire nei modelli di servizio *cloud* .

[117] Ove il titolare è il soggetto a cui è riservato ogni potere decisionale con riguardo alle finalità ed alle modalità del trattamento dei dati; mentre il responsabile rappresenta il soggetto a cui il titolare delega alcune specifiche operazioni di trattamento, sulla base di istruzioni impartite dal titolare stesso.

Nello specifico, le figure di rilievo sono: il *cloud provider* , che acquisisce e gestisce le infrastrutture di elaborazione necessarie a 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.

Da ciò emerge un forte frazionamento dei ruoli che, unito alla natura stessa del servizio reso, comporta un grado di autonomia dei singoli operatori, anche intermedi, assolutamente incompatibile con il

ruolo di meri, singoli, esecutori delle istruzioni impartite dal titolare, con una conseguente difficoltà in ordine alla concreta individuazione delle responsabilità e degli obblighi soggettivi di ognuno.

Proprio per questo motivo, in una società in cui i dati saranno sempre più spesso custoditi da soggetti terzi, parrebbe necessario un intervento normativo volto a riordinare l'attuale situazione di incertezza e a ridistribuire i pesi di responsabilità tra i diversi *player*, attraverso l'introduzione di una speciale figura di responsabile, che - a fronte di una sfera di autonomia particolarmente ampia, come quella occorrente per la gestione della nuvola - sia in grado di offrire ai clienti particolari garanzie in termini di affidabilità e di assumersi in prima persona specifiche responsabilità. Sarebbe auspicabile, tra l'altro, una individuazione a livello europeo di garanzie minime alla cui offerta dovrebbero essere obbligati tutti gli operatori che intendano affacciarsi sul mercato dei servizi di *cloud*, così come avviene in altri settori di particolare importanza, come ad esempio il settore bancario ed il settore assicurativo, i quali presentano dei regolamenti *ad hoc* data la rilevanza dei rischi sottesi alle attività svolte,

che non è lecito trascurare. Certamente l'imposizione di vincoli regolamentari non frenerà - e nemmeno deve farlo - lo sviluppo del *cloud*, tuttavia la certificazione della affidabilità del provider può certamente rappresentare un passaggio necessario al fine di creare nel mercato quelle condizioni di fiducia che consentano di vincere le resistenze anche dei soggetti più cauti nell'affidarsi alla nuvola.

3.2 Violazione del contratto e risarcimento del danno

Tutto ciò premesso, data l'importanza dei beni oggetto dei servizi di *cloud*, sarà facilmente comprensibile come l'implicazione più rilevante ricollegata all'uso dei servizi stessi di *cloud* sia data dall'ipotesi dell'inadempimento contrattuale; fondamentale sarà, altresì, stabilire con chiarezza e sicurezza fino a che punto debba estendersi l'eventuale obbligo risarcitorio e a quale entità ammonti. Gli schemi contrattuali normalmente adottati nel settore pongono particolare attenzione al tema dell'esonero ovvero della limitazione della responsabilità, anche perché, come già osservato, in ambiente *cloud* un problema nell'erogazione del servizio o nella sicurezza ed

integrità dei dati finisce inevitabilmente per ripercuotersi su un gran numero di utenti, se non addirittura su tutti.

La questione diventa ancora più seria quando si tratta di dati ed informazioni aziendali riservate che costituiscono un vero e proprio bene immateriale su cui il titolare può vantare e, di fatto, esercitare, dei diritti dominicali[118]. Il tema è significativo; eventuali falle nella sicurezza dei dati

[118] Cfr. G. COLANGELO, *Diritto comparato della proprietà intellettuale*, Bologna, 2011, pag. 270.; G. RIZZO, *La responsabilità contrattuale nella gestione dei dati nel cloud computing,* relazione presentata al Convegno *"Cloud Computing e diritto – questioni attuali e sfide future"* organizzato dall'Università Commerciale L. Bocconi, Milano, 17.05.2012, il quale in particolare osserva come in Italia, infatti, siano tutelate come bene giuridico (si guardi l'art. 98 del decreto legislativo 10 febbraio 2005, n. 30 , Codice della proprietà industriale. La norma rafforza notevolmente la protezione già accordata alle informazioni aziendali riservate dall'art. 6-bis del Regio decreto 29 giugno 1939, n. 1127 - legge invenzioni- . Gli elementi costitutivi della fattispecie sono esattamente quelli contemplati dall'art. 39 dell'Accordo TRIPs - Agreement on Trade-Related Aspects of Intellectual Property Rights, firmato a Marrakesh, Marocco, il 15 aprile 1994 nel quadro dell'Uruguay Round - che costituisce la matrice internazionale della norma interna e di quelle, analoghe, adottate da svariati Paesi.) le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali che abbiano le seguenti caratteristiche: (a) siano segrete (in quanto non siano note o facilmente accessibili agli operatori del settore) ; (b) abbiano un valore economico in quanto segrete (il valore economico delle informazioni in questione deve derivare dal carattere segreto delle stesse nel senso che se divenissero di pubblico dominio le caratteristiche intrinseche delle medesime non sarebbero sufficienti a conservare il loro valore patrimoniale per l'impresa detentrice); (c) siano sottoposte a misure di segretezza adeguate da parte delle persone al cui legittimo controllo sono soggette. Dal punto di vista comparatistico, la disciplina interna in tema di segreto aziendale appare simile a quella statunitense sancita dall'Uniform Trade Secrets Act del 1979 che, ai fini dell'esercizio del diritto, richiede al soggetto leso di dimostrare che le informazioni siano state acquisite da terzi illegalmente (misappropriation) e cioè mediante improper means o breach of confidence. Nel Regno Unito, pur in assenza di un provvedimento legislativo specifico sui segreti aziendali che qualifichi gli stessi come un bene di proprietà intellettuale, la giurisprudenza sembra orientata decisamente nel senso di dare tutela al titolare delle informazioni in tutti i casi in cui vi sia stata una indebita o illegittima appropriazione ed utilizzazione delle stesse.

archiviati, soprattutto se di questa natura, potrebbero causare addirittura l'azzeramento del valore economico di interi *assets* aziendali e, così, cagionare un danno competitivo all'utente del servizio[119], in special modo quando sia un imprenditore. Ma la violazione della sicurezza dei dati relativi all'utente potrebbe rilevare anche quando essa abbia ad oggetto dati privi dei requisiti per poter essere qualificate come informazioni aziendali riservate, oggetto di un diritto assoluto di natura dominicale. È il caso della c.d. *privacy* delle persone giuridiche. In linea di massima il debitore inadempiente è sempre responsabile dei danni diretti e prevedibili. Il problema più delicato è invece quello dei danni indiretti ed imprevedibili, che,

oltre ad essere di gran lunga più complesso, potendo portare ad potenziale indiscriminato ampliamento della responsabilità, è anche affrontato in maniera diversa dai vari sistemi giuridici. È questa la ragione per cui, prima di redigere una clausola di esonero o di

[119] L'impresa che vede irrimediabilmente leso il diritto assoluto sui propri dati aziendali, infatti, perde di norma anche la posizione di vantaggio concorrenziale che il possesso ed uso esclusivo di tali dati comporta.

limitazione dalla responsabilità, è opportuno conoscere con esattezza la disciplina applicabile.

In Italia, come noto, in caso di inadempimento o di ritardo nell'adempimento il debitore è tenuto a risarcire il creditore di tutti i danni prevedibili al momento in cui è sorta l'obbligazione, a meno che l'inadempimento non derivi da dolo del debitore[120]. Analoga impostazione restrittiva mostrano la legge francese e belga. Anche la maggioranza delle aree di *common law* sembrano improntata al medesimo criterio, per la verità di derivazione romanistica, della prevedibilità del danno[121].

Nel diritto tedesco e scandinavo, invece, vige la dottrina della "causalità adeguata" secondo cui deve essere risarcito qualunque danno che derivi in modo adeguato da un inadempimento contrattuale. In base all'art. 74 della Convenzione di Vienna sulla compravendita internazionale di merci[122] "il risarcimento del danno per l'inadempimento del contratto da parte di un contraente consiste in una somma uguale alla perdita, incluso il

[120] Art. 1225 cod. civ.

[121] Come enunciato nei principi della notissima sentenza Hadley-Baxendale.

[122] Convenzione delle Nazioni Unite sui Contratti di Compravendita Internazionale di Merci, adottata a Vienna l'11 aprile 1980, ratificata dall'Italia con Legge 11 dicembre 1985, n. 765.

mancato guadagno, subita dall'altro contraente in conseguenza dell'inadempimento. Il risarcimento del danno non può essere perdita che la parte inadempiente aveva previsto o avrebbe dovuto prevedere al momento della conclusione del contratto avuto riguardo ai fatti e alle circostanze che egli allora conosceva o avrebbe dovuto conoscere come possibile conseguenza dell'inadempimento". Secondo i principi Unidroit "il creditore ha diritto al risarcimento integrale del danno subito in conseguenza dell'inadempimento. Il danno comprende sia ogni perdita sofferta che ogni mancato guadagno, tenuto conto dei vantaggi economici che il creditore ha ottenuto evitando spese e danni" [123] con la precisazione che "la parte inadempiente è responsabile solo per il danno che ha previsto o poteva ragionevolmente prevedere al momento della conclusione del contratto come possibile conseguenza dell'inadempimento". Rispetto ad un contesto che, fatte salve alcune divergenze, appare improntato al criterio della prevedibilità del danno, corre l'obbligo di segnalare il par. 2-719 dello *Uniform Commercial*

[123] Art. 7.4.2.

Code statunitense secondo cui "*consequential damages may be limited or excluded unless the limitation or exclusion is unconscionable*"[124].

3.3 Soluzioni assicurative contro i rischi derivanti dall'utilizzo dei servizi cloud

Il tema della responsabilità del *cloud service provider* ha di recente interessato in maniera assai significativa anche il mondo delle assicurazioni. Sempre in tema di responsabilità del *cloud service provider*, una breve notazione merita la risposta del mercato assicurativo alla crescente domanda di servizi sulla nuvola. Molte compagnie assicurative, infatti, hanno sviluppato prodotti specifici, eliminando per altro verso la copertura per danni connessi alla perdita di dati e per violazioni alla riservatezza nei sistemi elettronici dalle normali polizze di responsabilità civile. Sono nate quindi delle polizze generalmente denominate "errori e omissioni tecnologici" , le *Tech E&O*, che possono essere sottoscritte sia dall'utente del servizio *cloud* sia dal *provider*. È bene tuttavia evidenziare che, allo stato dell'arte, la maggior parte di tali polizze esclude la copertura per danni della cui responsabilità l'assicurato si sia fatto volontariamente carico in via

[124] Cfr. G. RIZZO, *op. cit.*

contrattuale, così che - qualora il contratto con il cliente ne prevedesse - sarà necessario negoziare con la compagnia delle espresse eccezioni. Esistono poi delle soluzioni ibride di polizze *Tech E&O* e *Cyber Liability* che assicurano sia l'esposizione verso terzi sia quella verso la propria controparte contrattuale, coprendo una serie di costi come le spese di notifica della violazione, i servizi di monitoraggio e l'interruzione del servizio nonché servizi aggiuntivi come tutela legale specialistica, copertura di spese di perizie tecniche e di indagini, supporto nelle pubbliche relazioni, supporto IT[125].

[125] Cfr. G. RIZZO, *op.cit.*

4. *Le nuove frontiere: il cloud e la Pubblica Amministrazione*

Sull'onda delle scelte statunitensi[126] e su sollecitazione dei diversi *vendors*, anche la Pubblica Amministrazione italiana si è apprestata a spostare parte dei propri servizi in ambito *cloud*[127]. Nel corso degli ultimi anni è decisamente aumentato l'uso che le Amministrazioni italiane di ogni livello fanno delle nuove tecnologie; ciò per un duplice ordine di motivi: migliorare le *performances* e ridurre i costi utilizzando appieno l'evoluzione dell'informatica e del Web[128].

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

In verità, servirsi della nuvola nella PA non deve significare solo adottare una nuova e più conveniente infrastruttura tecnologica ma deve essere piuttosto una scelta consapevole verso una minore burocratizzazione

[126] Primi tra tutti, gli USA hanno già da tempo una vera e propria strategia nazionale sul *cloud computing* nel settore pubblico; cfr: http://www.cio.gov/documents/Federal-*Cloud*-Computing-Strategy.pdf.

[127] Così A. MANTELERO, "*Se l'Amministrazione va sulle nuvole: cenni ai profili legali ed ai modelli organizzativi del cloud computing per la PA",* in articolo pubblicato su Medialaws-Law and Policy of the Media in a Comparative Perspective.

[128] L'acquisizione di beni e servizi informatici in ambito pubblico è attività sempre più complessa, anche in considerazione della rapidissima evoluzione delle tecnologie; sotto questo profilo, è di sicuro interesse per gli Enti l'attività svolta da DigitPA in relazione alle "Linee guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione" la cui documentazione è disponibile a questo indirizzo: http://www.digitpa.gov.it/node/26.

dei processi decisionali e, quindi, una potenziale trasformazione delle modalità di interazione proprio tra PA, cittadini e imprese, in direzione una maggiore trasparenza e partecipazione e di un miglioramento dei offerti.

Il *cloud computing*, nelle diverse applicazioni che abbiamo analizzare e descrivere, potrebbe rappresentare una buona soluzione sia ai fini dell'adeguamento delle singole pubbliche amministrazioni al dettato dell'art. 50-*bis del CAD* - continuità operativa e *disaster recovery* [129]- , 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 prima ancora del Codice dell'Amministrazione Digitale - sono obbligate a rendere accessibili ai cittadini i propri servizi in modalità telematica, seppur

[129] Il Codice dell'Amministrazione Digitale prevede, all'articolo 50-bis, la c.d. "Continuità operativa", che tutte le Amministrazioni predispongano un piano di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività. L'attuazione della norma vede l'Agenzia per l'Italia Digitale in un ruolo centrale. Infatti, in sintesi, AgID è chiamata a definire le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, a verificare annualmente il costante aggiornamento dei piani di disaster recovery e informare annualmente il Ministro per la pubblica amministrazione e l'innovazione dell'esito di queste verifiche, ad emettere pareri sugli studi di fattibilità propedeutici alla produzione dei piani di continuità.

molto spesso non dispongano di adeguate risorse *hardware* e *software* al loro interno.

Sempre più spesso 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[130].

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.

[130] 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.

Sulla questione anche l'Unione Europea sta accelerando i tempi, ponendo come fulcro della propria Agenda Digitale la diffusione del *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*[131], 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

[131] European Cloud Partnership – ECP.

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[132]. 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.

Tuttavia, se è vero che, come fin qui detto, il *cloud* nella PA risolverebbe molti problemi pratici e normativi, le criticità tipiche dei servizi di *cloud* delle quali tanti abbiamo parlato fanno da barriera alla piena

[132] 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*.

affermazione di questo utilissimo e innovativo servizio all'interno della Pubblica Amministrazione; prevedere l'implementazione dei sistemi di *cloud* nella pubblica amministrazione, infatti, se da una parte può consentire l'immediato accesso ai servizi e la realizzazione della tanto agognata 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 e perciò, comprensibilmente, di estrema importanza. Riservatezza dei dati, responsabilità del fornitore, livelli minimi di sevizio, titolarità dei dati e delle informazioni diventa perciò, in questa sede, questioni ancor più significative e rilevanti e addirittura si arricchiscono di numerose sfumature e problematiche che meriterebbero un esame autonomo, tale è la loro ampiezza.

Se il *cloud*, rappresenta una sicura risorsa per una maggiore efficienza nell'amministrazione dei servizi pubblici, le pubbliche amministrazioni dovranno però, di volta in volta, valutare seriamente

la possibilità di gestire ed archiviare i propri documenti attraverso sistemi di conservazione basati su tecnologie *cloud*. 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 nazionalità che connotano questa tecnologia.

Così come per il settore privato infatti, anche per la Pubblica Amministrazione le principali criticità del ricorso al *cloud computing* sono indubbiamente rappresentate dalle implicazioni in materia di riservatezza e sicurezza dei dati trattati dagli Enti nell'esercizio della propria attività istituzionale; nel caso in cui siano i dati di una pubblica amministrazione a essere trasferiti *in the cloud*, occorre considerare, come appena anticipato, 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 problema della sicurezza è uno degli aspetti principali di tutti i sistemi informativi ma, se possibile, è ancora più importante nel pubblico: le Pubbliche Amministrazioni nell'esercizio della propria attività istituzionale raccolgono, producono ed archiviano un'enorme quantità di dati e documenti la cui riservatezza è fondamentale. Si tratta di un vero e proprio patrimonio che deve essere tutelato per mantenere l'integrità, e quindi l'affidabilità, delle informazioni pubbliche, prevenire e limitare i danni da intrusioni e accessi abusivi ed evitare possibilità di diffusioni non autorizzate di informazioni[133]; il primo aspetto che dovrà essere vagliato con attenzione riguarderà dunque 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[134] 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

[133] Così E. BELISARIO, *"Cloud Computing" , Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011, pag. 27 e ss.
[134] Art. 21, c.3 D.Lgs 42/2004.

giuridiche[135]. 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.

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[136]; il dovere di rendere accessibili i documenti cessa solo quando viene meno l'obbligo di

[135] 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).

[136] Artt. 22 e 23 L. 241/1990, modificata dalla L. 11 febbraio 2005, n.15. Ciò 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)

detenerli[137]. 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[138]che le Regole tecniche[139] prevedono la possibilità di acquisire tali servizi da fornitori esterni. Ovviamente resterà sempre in

[137] Art. 22, comma 6, L. 241/1990.
[138] D.Lgs. 82/2005.
[139] Di cui al DPCM 3 dicembre 2013.

capo alla singola amministrazione l'obbligo di selezionare accuratamente il fornitore e di verificarne l'operato[140].

Infine, rimane da specificare come le modalità di gestione del dato 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 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 alla gestione dei dati di rilievo pubblicistico, del cui trattamento la stessa PA è titolare e nell'erogazione di taluni servizi, soprattutto di natura certificativa, che sembra possibile in alcuni casi configurare una qualifica di incaricato di

[140] 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.

pubblico servizio per il *cloud provider* che sia fornitore di una pubblica amministrazione[141].

[141] Cfr. S.UNGARO, A.LISI, *Le 5 W del Cloud Computing*, e-book, Digital &Law Department.

CONCLUSIONI

L'indagine svolta fino a questo punto ci consente di poter concludere con qualche breve considerazione, a metà tra il finito e l'indefinito, un po' come tutta la tematica sottesa all'argomento che si è cercato di analizzare.

La crescente importanza assunta negli ultimi anni dalla tecnologia del *cloud computing* è la testimonianza di una interdipendenza fortissima tra società, mercato, economia da una parte e servizi tecnologico-informatici dall'altra, con una palese soccombenza, in termini di necessità, dei primi soggetti rispetto alla secondo categoria.

La testimonianza di una simile circostanza è facilmente riscontrabile nel massiccio numero di fornitori innanzitutto, che affacciandosi sempre più numerosi su questo nuova fetta di mercato dei servizi tecnologici, hanno calamitato l'attenzione delle imprese e dei privati consumatori innanzitutto, ma anche degli studiosi del settore, dei giuristi e dei sociologi, proprio per il forte impatto che la diffusione di questo nuovo strumento IT sta avendo e potrà avere sulla vita concreta di ognuno di noi.

Come ampiamente osservato, uno dei principali motivi del successo del *cloud computing* è rappresentato dalla circostanza che questa tecnologia permette di superare molte delle inefficienze tipiche dei sistemi informatici utilizzati fino a tempi piuttosto recenti, unito alla straordinaria versatilità - spaziando dall'uso domestico a quello aziendale del *cloud* - semplicità ed economicità dei servizi offerti.

Tuttavia, molti restano i punti oscuri in ordine all'utilizzo ed alla erogazione dei servizi di *cloud computing*; dalla regolamentazione dei rapporti contrattuali tra fornitore e utente all'individuazione della legge applicabile, nonchè alle implicazioni in materia di trattamento dei dati personali. Si tratta di temi di centrale importanza per il futuro sviluppo del *cloud*.

La necessità di sviluppare, sotto l'aspetto giuridico normativo, un'ampia strategia comune europea sul *cloud computing* è stata bene evidenziata dall'Agenda della Commissione Europea sul Digitale. La Commissione infatti, in una recente comunicazione al Parlamento[142], ha individuato il *cloud computing* - unitamente ai *social network* - tra i

[142] "A comprehensive approach on personal data protection in the European Union".

fenomeni emergenti che rendono non più differibile una radicale revisione del quadro normativo comunitario in materia di *privacy*, al fine di adeguare le regole e le categorie giuridiche esistenti ai nuovi modelli di condivisione e di gestione dei dati personali, il cui sviluppo ha di fatto scardinato la capacità di tenuta dell'impianto normativo esistente.

Ad ogni modo, in attesa di interventi che adattino la normativa esistente in materia di *privacy* alle sfide che il mercato pone nel settore del *cloud computing*, i maggiori e più rilevanti fattori di competitività per i *provider* potrebbero essere individuati proprio nella trasparenza, sia al momento della instaurazione della relazione contrattuale sia in costanza di rapporto; nell'offerta di adeguate garanzie in termini di misure di sicurezza; nell'offerta di adeguate garanzie patrimoniali per il caso di accesso abusivo, sottrazione o perdita dei dati.

Nel nostro Paese, il Garante per la protezione dei dati personali, dopo aver ammonito sui rischi di tali servizi, ha posto il *cloud computing* al centro della propria attività ispettiva per il 2011 ed il 2012[143]. Finora, però,

[143]http://europa.eu/rapid/pressReleasesAction.do?references=SPEECH/11/50&format=HTML&age nd=0&language=EN&guiLanguage=en;http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?fo

l'interesse delle istituzioni non si è tradotto in norme specifiche sulla "nuvola" e sui fenomeni e sulle conseguenze ad essa collegati e quindi problemi andranno risolti sulla base delle norme già vigenti nel nostro ordinamento, anche se non dettate con specifica attenzione per questa tecnologia. Ciò rappresenta, di per sé, una criticità, a cui si deve aggiungere che, come visto, il *cloud computing* nasce allo scopo precipuo di garantire la condivisione di tutto ciò che, in esso, viene importato. L'intervento del legislatore sarà, perciò, tanto indispensabile quanto inevitabile.

---

lderpath=Attivit%E0+dell%27Autorit%E0%2FRelazioni+annuali+al+Parlamento%2F2009; http://www.garanteprivacy.it/garante/doc.jsp?ID=1786472.

Bibliografia essenziale:

- U. Arnold, "New dimensions of outsourcing: a combination of transaction cost economics ande the core competencies concept", in European Journal of Purchasing & Supply Management, n. 6 (1), 2000;

- Bradshaw, Millar e Walden, "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services", Queen Mary University of London, School of Law, Legal Studies Research Paper No. 63/2010;

- S. Benucci, "Le prime pronunce in tema di «abuso di dipendenza economica"», in Vettori (a cura di), Concorrenza e Mercato;

- S.Bendani, Software as a Service (Saas): aspetti giuridici e negoziali, in http://www.altalex.com/index.php?idnot=44076;

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

- G. Buttarelli, "Verso un diritto della sicurezza informatica", in Riv. Sicurezza e informatica, Roma, 1995;

- F. Cardarelli, " La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing", in Dir. dell'Infirmazione e dell' Informatica, 1993, I, 86;

- G. Colangelo, "L'abuso di dipendenza economica tra disciplina della concorrenza e diritto dei contratti – Un'analisi economica e comparata", Torino, 2004;

- G. Colangelo, " Diritto comparato della proprietà intellettuale", Bologna, 2011;

- N.Fabiano, "I nuovi paradigmi della rete. Distribueted computing, cloud computing e "computing paradigms":abstract sugli aspetti e profile giuridici", in http://www.diritto.it/art.php?file=/archivio/27973.html;

- G. Finocchiaro, "Privacy e protezione dei dati personali. Disciplina e strumenti operativi", Bologna, 2012;

- H. Hoofnagle, "Consumer Protection in Cloud Compunting Services", Atti del convegno organizzato da Consumer Federation of America il 20-22 giugno 2010 alla New York University School of Law, successivamente pubblicato in Consumatori, Diritti e Mercato, 1/2011;

- M.G.. Losano , "Informatica Giuridica", in Dig. Civ., IX, Torino, 1993;

- A. Mantelero , "Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali", in Dir. Inf., 2010;

- A. Mantelero, "Se l'Amministrazione va sulle nuvole: cenni ai profili legali ed ai modelli organizzativi del cloud computing per la PA", in articolo pubblicato su Medialaws-Law and Policy of the Media in a Comparative Perspective;

- A. Mantelero, "Privacy digitale", in Manuale di informatica giuridica e diritto delle nuove tecnologie, a cura di Durante e Pagallo, Torino, 2012;

- A. Mazziotti di Celso, "Abuso di dipendenza economica", in G. Alpa – A. Clarizia (a cura di), "La Subfornitura, Commento alla legge 18 giugno 1998, n. 192", Milano, 1999;

- R. Marchini, "Cloud Computing: a Practical Introduction to the Legal Issues", London, 2010;

- A. Musella, "Il contratto di outsourcing del sistema informativo", in Dir. dell' Informazione e dell'Informatica, 1998;

- V. Pinto, "L'abuso di dipendenza economica «fuori dal contratto» tra diritto civile e diritto antitrust", in Riv. dir. civ., 2000;

- F. Prosperi, "Il contratto di subfornitura e l'abuso di dipendenza economica. Profili ricostruttivi e sistematici", Napoli, 2002;

- G. Rizzo, "La responsabilità contrattuale nella gestione dei dati nel cloud computing", relazione presentata al Convegno "Cloud Computing e diritto, questioni attuali e sfide future", Università Commerciale L. Bocconi, Milano, 17.05.2012;

- S. Ungaro, A.Lisi, "Le 5 W del Cloud Computing", e-book, Digital &Law Department, 2014;

- D.F. Parkhill, " The Challenge of the Computer Utility", Reading Mass., 1966;

- O.E Williamson, "Markets and Hierarcjies; Analysis and Anti-Trust Implication", New York, 1975e Clouds: Towards a Cloud Definition", Vol. 39, N. 1, January 2009;

- Wieder, Butler, Theilmann and Yahyapour, "Service Level Agreements for Cloud Computing", Springer, 2011;

- A. Zincone, " Il contratto di outsourcing: natura, caratteristiche, effetti", in Dir. aut., 2002.