## CLOUD COMPUTING E NON DISCLOSURE AGREEMENT

## 1. IL CLOUD COMPUTING : DEFINIZIONE, MODELLI E ANALISI NORMATIVA

**1.1.** Il cloud computing è un modello basato sulla disponibilità ubiqua, conveniente e on-demand di risorse condivise e configurabili (quali servers, storage, applicazioni, ecc.) che possono essere rapidamente preparate e messe a disposizione con un elevato grado di automazione. In altri termini, si tratta di una modalità per fornire tecnologie e risorse informatiche attraverso una rete, tipicamente Internet, con un sistema scalare, cioè flessibile, a seconda delle esigenze degli utenti.

Secondo la definizione di cloud computing del NIST (National Institute of Standards and Technology americano), il cloud computing è un modello per abilitare l'accesso on-demand e da qualsiasi punto a un pool di risorse computazionali condivise, come capacità computazionale, di storage o capacità di networking, che possono essere rese disponibili e rilasciate rapidamente con un minimo sforzo di gestione da parte del fornitore del servizio.

**1.2.** La tecnologia Cloud prevede vari modelli di servizio ed esattamente:

- Il Private cloud: un'infrastruttura ICT dedicata ai servizi richiesti da una singola organizzazione. Si tratta quindi in sostanza di un tradizionale centro di elaborazione dati (data center), nel quale però grazie a tecniche di virtualizzazione si consegue l'ottimizzazione in fatto di uso delle risorse disponibili.
- Il Public cloud, l'infrastruttura, invece, è di proprietà di un fornitore specializzato nella fornitura di servizi, il quale mette a disposizione di consumatori finali le relative risorse informatiche, che vengono quindi condivise tra loro. Con tale infrastruttura l'utente cede una parte importante del controllo esercitabile su di essi.
- L'Hybrid cloud, dove i servizi erogati da infrastrutture private coesistono con servizi acquisiti da cloud pubblici.

La flessibilità e la semplicità con cui è possibile configurare i sistemi in CLOUD ne rende possibile un dimensionamento "elastico", ossia adeguato alle esigenze specifiche secondo un approccio basato sull'utilizzo. Esistono vari modelli di erogazione del servizio CLOUD richiesto da un utilizzatore.

A seconda poi delle esigenze dell'utente in ordine al tipo di servizio informatico richiesto, sul mercato sono disponibili varie soluzioni di CLOUD computing, sia in ambiente CLOUD privata che pubblica, che ricadono in linea di massima in tre categorie, o modelli di erogazione del servizio:

- Software as a Service, ossia SaaS.

Un fornitore cloud può fornire l'accesso a proprie applicazioni software, quali E-mail, backup, o strumenti di produttività nell'ufficio (ad esempio elaborazione di fogli di calcolo o di testi, gestione del protocollo), nel qual caso si parla di modello di servizio SaaS.

- Platform as a Service, ossia PaaS.

Il fornitore può mettere a disposizione dei clienti cloud via Internet un ambiente costituito da

linguaggi di programmazione e software intermedi (middleware) nel quale essi possano sviluppare, far funzionare e gestire propri programmi applicativi, e si tratta allora del modello PaaS.

- Infrastructure as a Service, ossia IaaS..

Infine può essere fornito ai clienti accesso di rete, solitamente via Internet, alle funzioni di elaborazione dati, di archiviazione su memorie di massa, alle reti e ad altre fondamentali risorse informatiche, quale alternativa ai loro sistemi computazionali aziendali. Si tratta del modello IaaS.

**1.3.** In merito alla natura giuridica del contratto di cloud computing si devono evidenziare tre diversi orientamenti;

a. Contratto innominato

b. Contratto misto

c. Collegamento negoziale

La tesi prevalente è nel senso di ricostruire la fattispecie del cloud computing come un'ipotesi di collegamento negoziale che inizialmente è stata avanzata in relazione alla natura del contratto di fornitura di un sistema informatico ma che tuttavia, si ritiene applicabile anche al contratto di cloud computing.

Infatti, il contratto di appalto di servizi e il contratto di licenza risultano, piuttosto che formare un contratto misto, un insieme funzionalmente collegato. Ognuno dei contratti citati, singolarmente considerato, è inidoneo a realizzare l'operazione economica per la quale è stato concluso, ma nell'insieme essi sono volti a realizzare un'unica causa negoziale. In generale, più contratti si dicono collegati quando sussiste tra di essi un nesso di interdipendenza. Nel collegamento negoziale vi sono più contratti funzionalmente collegati: ad ogni contratto si applicherà la disciplina ad esso relativo.

**1.4.** In merito alle caratteristiche ed alla struttura dei contratti di cloud computing si osserva che detti vengono, normalmente, disciplinati attraverso contratti standard connotati da una assai limitata negoziabilità delle clausole e senza che si preveda un'eventuale rinegoziazione delle stesse. È stato osservato, inoltre, come nei servizi di cloud computing la maggiore asimmetria di forza esistente in favore del fornitore, unita al ruolo assunto in termini di conoscenza tecnologica, permette a quest'ultimo di imporre specifiche clausole contrattuali volte a consentire allo stesso, in maniera unilaterale, variazioni del servizio offerto o l'introduzione di innovazioni.

Da un punto di vista strutturale i contratti sono, solitamente, composti da più documenti ai quali manca, in molti casi, una coerente sistematizzazione della materia all'interno dei vari documenti e il medesimo aspetto viene disciplinato congiuntamente in documenti diversi.

I documenti formanti il contratto sono generalmente: A. Terms of Service (ovvero le condizioni generali di contratto), B. Service Level Agreement (SLA), C. Acceptable Use Policy (AUP) e D. Privacy Policy.

In particolare giova evidenziare l'importanza dei SLA e della Privacy Policy con riguardo alla

questione della tutela della riservatezza dei dati.

La Privacy Policy descrive l'approccio del fornitore nell'uso e protezione delle informazioni personali del fruitore del servizio: spesso contiene clausole specificatamente riguardanti la protezione dei dati personali. Sebbene sia normalmente presente un documento inerente le modalità di trattamento dei dati, lo stesso riguarda i molteplici servizi offerti dal provider, piuttosto che, specificatamente, il servizio cloud.

La mancanza di specificità nell'indicazione delle questioni relative al trattamento dei dati personali non è di poco conto.

Il Gruppo di lavoro per la tutela dei dati ex art. 29 nel Parere 05/2012 sul cloud computing ha, in effetti, evidenziato una serie di problematiche (tra le quali deve ricomprendersi anche la confidenzialità delle informazioni) che risultano raramente considerate nelle Privacy Policy dei cloud computing provider.

In primo luogo, i servizi di cloud computing possono comportare il coinvolgimento di una serie di parti contraenti che fungono da incaricati del trattamento. Inoltre, è comune che gli incaricati del trattamento designino dei sub-incaricati i quali ottengono l'accesso ai dati personali. Qualora vi sia un appalto dei servizi a sub- contraenti, gli incaricati del trattamento sarebbero tenuti ad informarne il cliente, descrivendo nel dettaglio il tipo di servizio concesso in subappalto, le caratteristiche dei subcontraenti attuali o potenziali e le garanzie offerte da queste entità al fornitore di servizi di cloud computing.

Altro aspetto posto in evidenza nel Parere 05/2012 riguarda l'obbligo del cloud provider di fornire un elenco dei luoghi ove viene effettuato il trattamento dei dati. Questa previsione pare scontrarsi con la mancanza di un'ubicazione stabile dei dati all'interno della rete del fornitore cloud. Infatti, i dati possono trovarsi in un centro di trattamento alle due del pomeriggio e dall'altra parte del mondo alle quattro del pomeriggio. Alla luce di questi rilievi, alcuni tra i principali cloud provider, per esempio Amazon, offrono “aree regionali” nelle quali viene assicurato permarranno i dati relativi all'utilizzatore del servizio.

## 2. RAPPORTO TRA CLIENTE E CLOUD PROVIDER

I servizi di cloud computing presentano delle criticità alle quali si deve porre particolare attenzione.

Il potenziale cliente dovrà avere la certezza sulla affidabilità e integrità del fornitore e sulla adeguatezza delle misure adottate per la protezione dei propri dati. Sarà necessario valutare attentamente le misure di sicurezza che il servizio offre, come la protezione delle strutture che ospitano i servizi, dell’hardware, del personale dedicato, nonché l'adozione di misure atte a proteggere il software a livello di sistema operativo, infrastruttura e applicazioni.

Le questioni che devono essere affrontate sono:

a) Non tutti i dati richiedono uguale tutela, quindi le imprese devono classificare i dati destinati a

essere immagazzinati all'interno di ambienti di Cloud storage e identificare eventuali obblighi di conformità in materia di notifica delle violazioni.

Si raccomanda, inoltre, che le imprese mettano in atto un piano di sicurezza aziendale dei dati che definisca i processi di business utili a gestire le richieste di accesso da parte delle autorità incaricate dell'applicazione delle leggi in materia di privacy e tutela dei dati.

b) Le imprese dovrebbero porre domande specifiche al provider di servizi Cloud, per determinare le modalità attraverso le quali vengono espletate tutte le formalità di tutela dei dati lungo il ciclo di vita dello storage.

Le imprese dovrebbero sapere, in particolare, se:

- Vengono utilizzate tecnologie di archiviazione multi-tenant e, nel caso, scoprire qual è il meccanismo di separazione in uso tra i diversi "inquilini" del condominio.
- Vengono utilizzati meccanismi di etichettatura (tag), per impedire che i dati vengano replicati in determinati paesi o regioni.
- Lo storage utilizzato per l'archiviazione e il backup sia dotato nativamente di tecnologie di crittografia e se la strategia di gestione delle chiavi include opzioni di strong authentication o di gestione delle policy di accesso, per limitarne l'accesso in determinate giurisdizioni.

Si raccomanda alle imprese di utilizzare la cifratura per implementare un sistema di gestione end-to-end del ciclo di vita dei dati, che contempli anche delle chiavi utili per distruggere digitalmente i dati giunti a fine vita, garantendo nel contempo che le chiavi non possano essere in alcun modo compromesse o replicate.

c) Come requisito minimo, si raccomanda alle imprese di assicurarsi di verificare che il CSP (fornitore di servizi Cloud) sostenga protocolli di comunicazione sicuri come SSL/TLS (Secure Socket Layer/Transport Layer Security) per l'accesso del browser o connessioni basate su VPN per l'accesso protetto ai suoi servizi.

Le aziende si dovrebbero sempre premurare di crittografare i dati sensibili in movimento verso il Cloud, ma se i dati risultano in chiaro durante l'uso o la conservazione, allora spetterà all'impresa ridurre le conseguenze di eventuali violazioni dei dati.

Nei contratti IAAS, si raccomanda che i service provider favoriscano la garanzia della separazione delle reti tra gli inquilini, in modo che un inquilino non possa mai vedere il traffico di rete di un altro.

d) Le imprese dovrebbero sempre mantenere al proprio interno la gestione delle chiavi di cifratura, ma qualora queste fossero gestite da un Cloud provider, è necessario per l'impresa controllare sempre che vengano assicurati controlli di gestione degli accessi in grado di soddisfare gli obblighi di notifica relativi alla paternità dei dati e alla violazione degli stessi.

Qualora le chiavi fossero gestite o disponibili nel Cloud, è assolutamente necessario che il fornitore sia in grado di assicurare uno stretto controllo sugli snapshot potenziali dei carichi di lavoro, per

evitare il rischio che i malintenzionati riescano ad analizzare il contenuto della memoria per ottenere le chiavi.

e) Si raccomanda alle aziende di obbligare il proprio fornitore di servizi Cloud a supportare sistemi di restrizione degli accessi alle sottoreti IP, in modo che le imprese siano in grado di limitare l'accesso degli utenti finali solo ad alcuni dispositivi o intervalli di indirizzi IP noti.

L'impresa dovrà, inoltre, pretendere che il provider delle tecnologie di cifratura sia in grado di garantire controlli amministrativi adeguati, tecnologie di strong autentication (come l'autenticazione a due fattori), gestione dei permessi di accesso e separazione delle funzioni amministrative quali la sicurezza e la manutenzione delle reti.

Le imprese dovrebbero anche pretendere:

- la registrazione di tutti gli utenti e l'accesso degli amministratori a tutte le risorse immagazzinate nel Cloud fornendo questi registri all'impresa in un formato immediatamente recepibile dai sistemi di gestione della sicurezza delle informazioni o degli eventi.
- che il CSP limiti a pochi soggetti altamente qualificati l'accesso agli strumenti di gestione dei sistemi particolarmente evoluti, tipo quelli che potrebbero creare un'istantanea (snapshot) dei carichi di lavoro in tempo reale, gestire la migrazione dei dati, eseguire il backup o ripristinare i dati.
- che le immagini acquisite con gli strumenti di migrazione o snapshot siano trattate con la stessa sicurezza degli altri dati aziendali sensibili.

f) Si consiglia alle aziende di comprendere sempre l'impatto dei sistemi di indicizzazione e codifica sulle applicazioni, i motori di ricerca e l'ordinamento dei database. Si dovrebbe prestare particolare attenzione a funzionalità avanzate di ricerca.

Se il fornitore di tecnologie di cifratura offre opzioni per preservare la funzione di crittografia i regolamenti nazionali potranno richiedere l'uso di algoritmi standardizzati e approvati o il parere di un ente di certificazione indipendente in merito all'eventuale adozione di sistemi di cifratura potenzialmente più deboli.

g) Nel corso degli ultimi dieci anni, è emerso un nuovo paradigma collegato alla crittografia a chiave pubblica che ha come obiettivi (i) la crittografia basata su attributi (attribute-based encryption, ABE), che permette il controllo degli accessi a grana fine e (ii) una sua generalizzazione, la crittografia funzionale, che permette la computazione selettiva sui dati cifrati. Più precisamente:

– nella crittografia basata su attributi, i dati criptati sono associati ad attributi ed a chiavi di decifratura segrete, insieme a regole che stabiliscono quali dati cifrati possono essere decriptati da quali chiavi. Ad esempio, un fornitore di contenuti digitali può stabilire che nei giorni feriali una data chiave di decifratura permette l'accesso ai contenuti standard e premium e l'accesso a solo quelli standard nei giorni festivi.

– nella crittografia funzionale, un utente in possesso di una chiave segreta può apprendere una

funzione specifica dei dati cifrati, e solo quella funzione. Ad esempio, la decriptazione di una colonna di valori numerici con una chiave corrispondente alla media aritmetica rivela il valore di tale statistica e niente altro.

Una caratteristica peculiare sia della crittografia basata su attributi sia di quella funzionale consiste nel fatto che possono esserci diverse chiavi segrete, ognuna con differenti capacità di decriptazione.

Il paradigma della crittografia funzionale (insieme al caso più specifico della crittografia basata su attributi) può essere inteso come una generalizzazione di casi più specifici di estensioni della crittografia a chiave pubblica apparse nel corso degli anni, quali la crittografia broadcast, la crittografia basata su identità, o la crittografia che permette l'esecuzione di interrogazioni direttamente sui dati cifrati (searchable encryption, SE). In retrospettiva, la maggior parte delle innovazioni nel campo della crittografia a chiave pubblica negli ultimi anni, possono essere considerate come casi speciali della crittografia basata su attributi, o crittografia funzionale.

Gli obiettivi che lo studio della crittografia sia basata su attributi sia funzionale sono quindi (i) la definizione di schemi di cifratura che possono esprimere un ampio insieme di politiche di accesso e funzioni, e (ii) la realizzazione di implementazioni (il più possibile) efficienti di tali schemi, basandosi su problemi computazionali che sono (quasi) universalmente ritenuti molto difficili da risolvere in modo efficiente. I più semplici esempi di schemi di cifratura basati su attributi sono i cosiddetti schemi basati sull'identità (identity-based encryption, IBE), dove sia il messaggio criptato sia la chiave segreta di decifratura sono associati a identità e la decifratura è possibile solo quando le due identità coincidono.

Nell'ultimo decennio, partendo dai primi schemi IBE, stati definiti molti schemi che hanno via via ampliato l'insieme delle politiche di accesso esprimibili e, contemporaneamente, sono state investigate molte tecniche che permettono la computazione di funzioni sempre più generali su dati cifrati.

Ovviamente, oltre alla definizione di schemi crittografici funzionali sempre più espressivi, è necessario fornire corrispondenti implementazioni che siano un compromesso ragionevole tra espressività, efficienza e sicurezza. Tali aspetti dipendono in modo cruciale dai problemi computazionalmente difficili da risolvere scelti come punto di partenza delle implementazioni.

*

Nell'ottica che qui interessa ovvero la necessità di proteggere la confidenzialità dei propri dati il cliente-utilizzatore dei servizi cloud deve attentamente valutare anche le misure di sicurezza adottate dal provider per consentire l'allocazione dei dati in cloud. E' essenziale che il provider preveda ed utilizzi tecniche di trasmissione cifrata dei dati in entrata ed uscita dal cloud con l'ulteriore cautela dell'adozione di meccanismi di identificazione dei soggetti autorizzati all'accesso ai dati nel cloud.

Il fondamentale bisogno di tutela della confidenzialità e riservatezza dei dati in cloud determina il

necessario impiego di tecniche di cifratura e crittografia sia in fase di trasmissione che di conservazione dei dati sui sistemi del cloud provider.

In funzione di quanto sopra, è opportuno valutare la sottoscrizione di un accordo di riservatezza con il fornitore del servizio cloud che contenga anche un impegno alla cifratura e riservatezza. Un possibile format di tale accordo è qui di seguito riportato. In alternativa, è opportuno comunque valutare che le medesime previsioni siano sufficientemente e sostanzialmente contentute nei contratti di fornitura del servizio stipulati con il cloud provider.

**Accordo di Riservatezza**

*- ".... premesso*

*- che la società ALFA cliente-utilizzatore dichiara di intrattenere rapporti d'affari riservati con società, attraverso i quali potrebbe venire a conoscenza, a titolo di esempio e senza che ciò possa costituire elemento di esaustività, di: dati commerciali, incluso strategie e fabbisogni, lancio di nuovi prodotti costi, informazioni finanziarie e contrattuali, nominativi di clienti e fornitori, etc; o dati tecnici, inclusi brevetti, anche in corso di registrazione, progettazioni e soluzioni di progettazione, capitolati di fornitura e d'opera, disegni tecnici, specifiche di materiali, performance, piani e modalità di controllo, sistemi di qualità e sicurezza aziendali, reclami, etc.;*

*- che i rapporti commerciali sopra richiamati possono determinare la redazione di contratti, atti e documenti contenenti informazioni confidenziali, ovvero segreti commerciali e/o industriali relativi alla società stessa ed alla sua attività, in ciò comprendendo anche quelli delle controllate/partecipate e dei partner commerciali;*

*- che detti contratti, atti e documenti potranno essere archiviati nelle infrastrutture cloud del provider BETA;*

*- che la società ALFA cliente-utilizzatore ed il provider cloud BETA per facilitare il libero scambio d'informazioni, concordano di sottoscrivere il presente ACCORDO DI RECIPROCA RISERVATEZZA che disciplinerà le modalità di divulgazione o il divieto di divulgazione delle informazione di cui il provider cloud sia venuto a conoscere a seguito del rapporto di fornitura del servizio cloud.*

*- che, poiché le informazioni e i documenti potenzialmente contenuti nel cloud hanno o possono avere carattere strettamente confidenziale e riservato, le Parti, con la sottoscrizione del presente Accordo intendono regolamentare gli obblighi di riservatezza.*

*TUTTO CIÒ PREMESSO, SI STIPULA E SI CONVIENE QUANTO SEGUE*

***1. DEFINIZIONI:***

***1.1. " Informazioni Riservate"****: significa ogni informazione contenuta negli atti, nei documenti e in ogni scritto disponibile ed archiviata in cloud. Tali informazioni includono, senza alcuna limitazione, a titolo meramente indicativo e non esaustivo: informazioni tecniche, finanziarie e d'affari, modelli,*

*contratti, accordi, dati riferibili ad appaltatori, fornitori, consulenti, soci, preventivi, progetti, proiezioni di mercato, software, raccolte di codici, carte, diagrammi logici, segreti di mercato, procedimenti, formule, grafici ed altri materiali, invenzioni, documentazione, know-how, forme, tecniche, disegni e schizzi, dati ed ogni altra informazione, ivi inclusa ogni informazione relativa ai prodotti/contenuti/canali/servizi/progetti tecnici ed editoriali, sia che si tratti di informazioni concernenti direttamente le parti contraenti sia che si tratti di informazioni concernenti e/o relative ad altre Società dello stesso gruppo societario, determinato ai sensi e per gli effetti dell'articolo 2359 del Codice Civile, ivi incluse le società controllate, controllanti, collegate, consociate e/o affiliate, sia, infine, che si tratti di informazioni concernenti e/o relative ad altri soggetti terzi, fermo restando il diritto di questi ultimi di autorizzare, laddove previsto, la divulgazione di informazioni.*

***1.2 "Provider cloud"*** *Società di terze parti che fornisce servizi di archiviazione, applicazioni, infrastruttura o piattaforma basati sul cloud.*

***2. OGGETTO***

***2.1*** *L'Accordo ha ad oggetto la regolamentazione dei diritti e degli obblighi delle Parti rispetto alle Informazioni Riservate", come sopra definite. .*

***3. OBBLIGHI***

***3.1. Non rivelazione***

*Il provider cloud BETA si impegna a garantire che nessun soggetto avente accesso a quanto contenuto nel cloud riveli o trasmetta a terzi informazioni riservate acquisite, ad eccezione di quanto enunciato o prescritto dalla Legge - ed a meno che la Società ALFA cliente-utilizzatore del cloud non lo consenta per iscritto,*

*Il provider cloud BETA si impegna a non rivelare a Soggetti Terzi, ad impedire che Soggetti Terzi possano venire a conoscere ed a non utilizzare in alcun modo ed in alcuna forma le informazioni ed i dati tutti contenuti nella documentazione posta in cloud da ALFA.*

***3.2. Rispetto della riservatezza***

*Il provider cloud BETA, informerà i propri impiegati che abbiano ricevuto Informazioni Riservate, in conformità a quanto innanzi disposto, che essi sono soggetti a tutte le restrizioni contenute nell'Accordo.*

*Nel caso in cui il provider cloud BETA non possa assicurare la conformità alle disposizioni del presente Accordo da parte del proprio personale dipendente o dei collaboratori e consulenti, il medesimo si impegna ad adottare tutte le misure necessarie a garantire che non siano rivelate Informazioni Riservate a detti soggetti e che gli stessi non abbiano comunque accesso alle Informazioni Riservate .*

*Il provider del cloud BETA sarà responsabile verso ALFA nel caso in cui i propri impiegati o qualsiasi altro soggetto venuto in possesso delle informazioni contenute nel cloud direttamente o*

*indirettamente rispetto agli accessi abilitati, divulghino Informazioni Riservate in violazione delle disposizioni dell'Accordo, qualora ne derivi un pregiudizio o un danno ad ALFA.*

***3.3. Cifratura e crittografia***

*Il provider cloud BETA prende atto, accetta e si impegna a che, data l'unicità della natura delle informazioni contenute nel cloud, l'allocazione nel cloud delle informazioni, dati, contratti e documenti debba avvenire con sistemi cifrati di trasmissione dati secondo la piu' evoluta tecnologia esistente e che la conservazione nel cloud delle informazioni, dati, contratti e documenti debba avvenire in modalità crittografata secondo la piu' evoluta tecnologia esistente".*

## 3. NON DISCLOSURE AGREEMENT E CLOUD COMPUTING NEI RAPPORTI TRA PARTNERS COMMERCIALI

L'accordo di riservatezza viene stipulato, in ambito professionale o fra privati, per proteggere determinate informazioni dalla divulgazione pubblica. Nel mondo degli affari questo genere di negozio è noto come NDA ovvero non disclosure agreement.

In linea di massima all'interno di un accordo di riservatezza le parti individuano le informazioni che intendono mantenere come confidenziali e si impegnano a non svelarle o comunque renderle accessibili a terzi.

Questo genere di accordo viene stipulato essenzialmente per proteggere i segreti industriali o aziendali, oppure per proteggere dati aziendali sensibili, o ancora per evitare la divulgazione di informazioni commerciali private.

Dovendo stilare un NDA la prima cosa da valutare è se entrambe le parti debbano mantenere il segreto, o se il non disclosure agreement limita una sola parte. La mutua limitazione è solitamente utilizzata quando due società commerciali si ritrovano a valutare la possibilità di un business comune.

Altro elemento essenziale di un accordo di riservatezza è certamente lo scopo: l'uso delle informazioni previste nel negozio giuridico può essere limitato alla realizzazione di un determinato obiettivo. Questa parte del contratto è molto importante e deve essere molto particolareggiata, perché la limitazione può essere in qualunque momento ampliata ma non ristretta.

Ogni Non Disclosure Agreement può essere composto su misura delle necessità delle parti: la durata può prevedere una scadenza stabilita oppure può essere a tempo indeterminato. Solitamente gli accordi senza scadenza contengono informazioni non brevettabili, liste clienti o informazioni sensibili la cui divulgazione danneggerebbe una delle parti coinvolte nel contratto.

L'ultima clausola che non può mancare all'interno di un NDA è quella che riguarda la possibilità o meno di condividere le informazioni sottoposte a confidenzialità all'interno del contratto con i propri collaboratori o i propri consulenti: il non rispetto di una clausola produce delle sanzioni stabilite all'interno del negozio giuridico stesso.

Oltre a contenere le parti e cosa debba essere considerato confidenziale, spesso in maniera anche

molto particolareggiata, un NDA contiene anche tutti i casi in cui la limitazione d'uso dei dati va a decadere.

Ovviamente le parti dovranno stabilire i termini di confidenzialità delle informazioni e la durata complessiva dell'accordo, ma anche quali libertà di divulgazione a terzi possiedono le parti.

Si è già detto in precedenza che è interesse ed onere del soggetto che richiede servizi di cloud computing verificare l'affidabilità e integrità del fornitore di tali servizi e la adeguatezza delle misure adottate per la protezione dei propri dati. Ciò nonostante, in considerazione del fatto che l'utilizzo del cloud computing comporta comunque una forma, per così dire, di "trasferimento" di dati al soggetto che rende tale servizio, benché sul presupposto della garanzia della loro non violabilità nonché del loro corretto stoccaggio solo ed unicamente ai fini per i quali il servizio è reso, si rende opportuno inserire nel NDA, sottoscritto con i propri partners commerciali, una specifica clausola che consenta espressamente l'utilizzo di Cloud services anche in relazione ai dati che formano oggetto del medesimo NDA.

In vista di ciò, si riporta qui di seguito una possibile formulazione di tale clausola:

"*fermi tutti gli obblighi di riservatezza contenuti nel presente accordo, le Parti precisano che è facoltà delle stesse, e pertanto loro consentito, utilizzare servizi di Cloud computing forniti da terzi al fine di stoccare i dati di qualsiasi tipo inerente la attività di ciascuna di esse, inclusi i dati e le informazioni confidenziali ricevuti dall'altra parte, oggetto del presente accordo di riservatezza. Sarà cura della parte che utilizza i detti servizi di Cloud computing verificare che il fornitore dei medesimi servizi abbia adottato e continui costantemente ad adottare adeguate misure per la protezione dei dati immessi.* "

## 4.. LA CRITTOGRAFIA E LA CIFRATURA NELL'ESPERIENZA ITALIANA E NELLA NORMATIVA EUROPEA

Se guardiamo alla normativa italiana, la crittografia compare come misura di sicurezza in numerosi provvedimenti del Garante (se ne citano alcuni senza pretesa di esaustività): si fa cenno alla cifratura nel Provvedimento su Sicurezza dei dati di traffico telefonico e telematico – 17 gennaio 2008, nel Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach) – 4 aprile 2013, nel Provvedimento in materia di misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica – 18 luglio 2013, nel Provvedimento generale prescrittivo in tema di biometria – 12 novembre 2014, nelle Linee guida sul dossier sanitario elettronico 4 giugno 2015, in quello in ordine alle Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche – 2 luglio 2015.

Non solo: il GARANTE raccomanda l'uso della crittografia anche nel cloud computing e vi accenna, seppure in modo informale, in ordine all'internet of things; il ricorso a tecniche di cifratura, infine, compare in molti provvedimenti tarati su casi concreti portati alla sua attenzione.

In ambito europeo la Direttiva 95/46/CE non faceva invece direttamente riferimento a tecniche di cifratura: l'articolo 17, rubricato "Sicurezza dei trattamenti" imponeva, in pratica, al Titolare l'attuazione di misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.

Una novità importante si ha con il Regolamento Europeo.

La crittografia, ad esempio, viene menzionata diverse volte nel Regolamento: si tratta di uno strumento di cui il titolare e il responsabile possono avvalersi per mitigare i rischi connessi ai trattamenti (fatto che, in ottica di accountability, va tenuto in adeguata considerazione).

Si fa riferimento alla crittografia ad esempio nel considerando n. 83 ove si dispone che "Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura". Il considerando viene poi tradotto nell'articolo 32 del regolamento medesimo, che, collocato nella sezione riferita alla sicurezza dei dati personali e rubricato sicurezza del trattamento dispone che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali" (…).

La pseudonimizzazione e la cifratura, pertanto, sono misure che devono essere tenute in debita considerazione quando si valutano i rischi di sicurezza ed in ottica di tutela della confidenzialità di dati, contratti, atti e documenti. Nella medesima sezione si trova anche l'art. 34, che, pure, menziona la crittografia. In particolare, l'articolo 34 disciplina la "Comunicazione di una violazione dei dati personali all'interessato", come illustra efficacemente la sua rubrica.

La cifratura esonera dal comunicare all'interessato il data breach.

Dal comma 3 lettera a) infatti si deduce che non è richiesta la comunicazione all'interessato se il titolare "ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura". I vantaggi sul piano dell'immagine aziendale e della competitività rispetto ai concorrenti potrebbero essere significativi.

Un riferimento alla cifratura è contenuto anche nell'articolo 6 del Regolamento, in ordine alla liceità del trattamento. Nel caso in cui il titolare raccolga dei dati personali ma voglia poi trattarli per una

finalità diversa da quella per la quale siano stati originariamente raccolti, e non abbia il consenso dell'interessato o non possa fondarsi su una norma di legge, dovrà valutare che questa seconda finalità sia compatibile con la prima. Per compiere questa valutazione il titolare del trattamento tiene conto, tra l'altro, a norma del comm 4 lettera e) "dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione"

Il ricorso alla cifratura, perciò, assume grande rilievo nell'ambito del Regolamento: e molto viene lasciato all'iniziativa dei titolari, in un bilanciamento che sarà certamente rilevante in termini di responsabilità.

Pertanto è possibile che si affermi come prassi consueta.

**Avv. Marco Del Fungo**