GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Cloud computing

Cloud computing: indicazioni per l'utilizzo consapevole dei servizi

Schede di documentazione

www.garanteprivacy.it

Cloud computing: indicazioni per l'utilizzo consapevole dei servizi

INDICE

1. PREMESSA

L'Autorità nell'ottica di promuovere un utilizzo corretto delle nuove modalità di erogazione dei servizi informatici, specie per quelli erogati tramite *cloud* pubbliche (*public cloud*), che comportano l'esternalizzazione di dati e documenti, ritiene opportuna e doverosa un'opera di informazione orientata a tutelare l'importante patrimonio informativo costituito dai dati personali.

Tali indicazioni si propongono, quindi, di offrire un primo insieme di indicazioni utili a tutti gli utenti di dimensioni contenute e di limitate risorse economiche (singoli, piccole o medie imprese, amministrazioni locali quali i piccoli comuni, ecc.) destinatari della crescente offerta di servizi di *cloud computing* (pubbliche o ibride), con l'obiettivo di favorire l'adozione consapevole e responsabile di tale tipologia di servizi.

Le avvertenze di seguito enucleate costituiscono un primo quadro di cautele che favoriscono il corretto trattamento dei dati personali attraverso l'utilizzo dei predetti servizi virtuali e, pertanto, si indirizzano anche ai fornitori, i quali possono fare riferimento a tali indicazioni nella predisposizione dei loro servizi, con l'accortezza di informare opportunamente gli utenti in ordine alla loro adozione.

L'Autorità - nella consapevolezza che l'utilizzo dei servizi di *cloud computing* prefigura problematiche ben difficilmente risolvibili a livello nazionale che richiedono, invece, una riflessione condivisa a livello sia europeo sia internazionale, e in considerazione di tutte le sue implicazioni in relazione al trattamento dei dati personali - intende in ogni caso continuare a seguire l'evoluzione del fenomeno, anche partecipando con altri decisori istituzionali a specifici tavoli di lavoro aperti in materia, in particolare con *DigitPA* per quanto attiene all'adozione di modelli orientati alle *cloud* in ambito pubblico. L'Autorità, inoltre, si riserva, laddove ne rilevasse la necessità, di adottare in futuro specifiche e dettagliate prescrizioni indirizzate a utenti e fornitori, specie sotto il profilo delle misure di sicurezza.

2. CHE COSA È IL *CLOUD COMPUTING*?

L'evoluzione delle tecnologie informatiche e dei mezzi di comunicazione è inarrestabile e ogni giorno vengono messi a disposizione dei cittadini nuovi strumenti e soluzioni sempre più sofisticate e integrate con la rete Internet, che consentono di soddisfare crescenti esigenze di informatizzazione e di comunicazione.

In tale quadro, il *cloud computing* è un insieme di modelli di servizio che più di altri si sta diffondendo con grande rapidità tra imprese, pubbliche amministrazioni e cittadini perché incoraggia un utilizzo flessibile delle proprie risorse (infrastrutture e applicazioni) o di quelle messe a disposizione da un fornitore di servizi specializzato. L'innovazione e il successo delle *cloud* (le nuvole informatiche) risiede nel fatto che, grazie alla raggiunta maturità delle tecnologie che ne costituiscono la base, tali risorse sono facilmente configurabili e accessibili via rete, e sono caratterizzate da particolare agilità di fruizione che, da una parte semplifica significativamente il dimensionamento iniziale dei sistemi e delle applicazioni mentre, dall'altra, permette di sostenere gradualmente lo sforzo di investimento richiesto per gli opportuni adeguamenti tecnologici e l'erogazione di nuovi servizi.

Nell'ambito del *cloud computing* è ormai prassi consolidata distinguere tra *private cloud* e *public cloud*.

Una *private cloud* (o nuvola privata) è un'infrastruttura informatica per lo più dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo (nella tradizionale forma dell'*hosting* dei *server*) nei confronti del quale il titolare dei dati può spesso esercitare un controllo puntuale. Le *private cloud* possono essere paragonate ai tradizionali *"data center"* nei quali, però, sono usati degli accorgimenti tecnologici che permettono di ottimizzare l'utilizzo delle risorse disponibili e di potenziarle attraverso investimenti contenuti e attuati progressivamente nel tempo.

Nel caso delle *public cloud*, invece, l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni - e quindi condivide tra di essi - i propri sistemi attraverso l'erogazione

via *web* di applicazioni informatiche, di capacità elaborativa e di stoccaggio. La fruizione di tali servizi avviene tramite la rete Internet e implica il trasferimento dell'elaborazione o dei soli dati presso i sistemi del fornitore del servizio, il quale assume un ruolo importate in ordine all'efficacia delle misure adottate per garantire la protezione dei dati che gli sono stati affidati. In questo caso l'utente insieme ai dati, infatti, cede una parte importante del controllo esercitabile su di essi. Ad esempio, la complessità delle infrastrutture, e la loro eventuale dislocazione su siti al di fuori dei confini nazionali potrebbe determinare l'impossibilità sia di conoscere con esattezza l'ubicazione dei propri dati nella nuvola, sia di sapere se e quando i dati vengono spostati da un luogo all'altro per esigenze organizzative, tecniche o economiche difficilmente determinabili e gestibili a priori. Inoltre, la dimensione del fornitore potrebbe condizionare la forza contrattuale dei fruitori del servizio e la loro possibilità di esercitare un controllo diretto, seppur concordato, sui siti e sulle infrastrutture utilizzate per ospitarne i dati.

Acquisire servizi *cloud* significa acquistare presso un fornitore di servizio risorse (ad esempio *server* virtuali o spazio disco) oppure applicazioni (ad esempio posta elettronica e strumenti per l'ufficio) • I dati non risiedono più su *server* "fisici" dell'utente, ma sono allocati sui sistemi del fornitore (a meno di copie in locale) • L'infrastruttura del fornitore del servizio è condivisa tra molti utenti per cui sono fondamentali adeguati livelli di sicurezza • L'utilizzo del servizio avviene via *web* tramite la rete Internet che assume dunque un ruolo centrale in merito alla qualità dei servizi fruiti ed erogati • I servizi acquisibili presso il fornitore del servizio sono a consumo e in genere è facile far fronte ad eventuali esigenze aggiuntive (ad esempio più spazio disco o più potenza elaborativa) • Esternalizzare i dati in remoto non equivale ad averli sui propri sistemi: oltre ai vantaggi, ci sono delle controindicazioni che bisogna conoscere

Tabella: Aspetti chiave legati al cloud computing erogato tramite cloud pubbliche

Accanto alle *private* e *public cloud* si annoverano nuvole "intermedie" quali le *cloud* ibride (o *hybrid cloud*), caratterizzate da soluzioni che prevedono l'utilizzo di servizi erogati da infrastrutture private accanto a servizi acquisiti da *cloud* pubbliche, e le *community cloud* in cui l'infrastruttura è condivisa da diverse organizzazioni a beneficio di una specifica comunità di utenti.

I potenziali vantaggi del *cloud computing* certamente possono promuovere la sistematizzazione delle infrastrutture, la riorganizzazione dei flussi informativi, la razionalizzazione dei costi e quindi in generale favorire nel caso sia del mondo imprenditoriale, sia della pubblica amministrazione servizi più moderni, efficienti e funzionali in linea con le esigenze di crescita di un moderno Sistema Paese. È d'altra parte assodato che il *cloud computing* non è un fenomeno temporaneo o una moda, ma il passo successivo dell'evoluzione nel modo in cui si utilizza la Rete Internet, che da strumento per la sola condivisione documentale (la pagina *web* resa disponibile dal sito *web* remoto) diviene la porta d'accesso alle risorse elaborative di un *provider* di servizi (l'applicazione resa disponibile in modalità *web*).

Questa trasformazione sta determinando una "modifica dei costumi" che è già in atto ed è più evidente nell'utenza individuale che più frequentemente, ma non sempre con completa consapevolezza anche dei possibili rischi derivanti dalle nuove tecnologie utilizzate, si avvale di servizi erogati da fornitori terzi (*public cloud*) per far fronte alle sue esigenze informative: l'utente *consumer*, infatti, utilizza i *social network* sui quali trasferisce abitualmente foto, informazioni, idee e opinioni, usa strumenti di elaborazione documentale via *web*, impiega gli *hard-disk* remoti per poter sempre disporre dei propri documenti da qualunque dispositivo e in qualunque luogo si trovi, si avvale delle applicazioni per i moderni smartphone sempre connessi ad Internet che tramite l'associazione delle informazioni di geolocalizzazione all'utente hanno aperto la strada a innovative funzionalità, anche in ambito sociale.

Risulta d'altra parte evidente come l'offerta degli operatori economici stia incalzando il mercato delle imprese e della Pubblica Amministrazione con soluzioni che incoraggiano l'acquisizione di servizi esternalizzati, utilizzando come volano verso

i nuovi investimenti la prospettiva di risparmi legati alla sostituzione o all'affiancamento degli *asset* per il trattamento delle informazioni tradizionalmente nel diretto possesso dell'utente, con soluzioni acquisite a consumo presso terzi.

È tuttavia opportuno evidenziare come il ricorso a quelle modalità che intrinsecamente promuovono l'utilizzo di servizi esternalizzati comportino anche la migrazione dei dati dai sistemi locali sotto il diretto controllo dell'utente, impresa o amministrazione ai sistemi remoti del *provider* di servizi.

3. ESTERNALIZZARE I DATI NELLE *CLOUD* PUBBLICHE

Come sopra delineato, le *public cloud* (o nuvole informatiche pubbliche) sono infrastrutture controllate da organizzazioni che le rendono disponibili a terzi attraverso la vendita di servizi a consumo. Lo spazio virtuale e la capacità di elaborazione della "nuvola" sono condivisi tra molti utenti, singoli o appartenenti a imprese o enti diversi che accedono a tali risorse dell'infrastruttura tramite l'utilizzo della rete Internet.

Più precisamente, con il termine *cloud computing* o semplicemente *cloud* nell'ambito di questo documento ci si riferisce a un insieme di tecnologie e di modelli di servizio che:

- favoriscono la fruizione e l'erogazione di applicazioni informatiche, di capacità elaborativa e di stoccaggio via *web*;
- promuovono a seconda dei casi il trasferimento dell'elaborazione o della sola conservazione dei dati dai *computer* degli utenti ai sistemi del fornitore dei servizi.

La flessibilità e la semplicità con cui è possibile configurare i sistemi in *cloud* ne rende possibile un dimensionamento "elastico", attuato cioè secondo logiche di adattabilità alle contestuali esigenze e di fruizione a consumo. Gli utenti non devono curarsi della gestione dei sistemi informatici che, essendo utilizzati secondo la logica dell'esternalizzazione (*outsourcing*), sono completamente gestiti dai soggetti terzi nella cui nuvola sono conservati i dati. Generalmente, nel caso frequente di fornitori di grosse dimensioni dotati di infrastrutture complesse, la nuvola può estendersi

geograficamente su siti distinti e l'utente potrebbe ignorare dove vengono effettivamente conservati i propri dati.

I servizi offerti dai fornitori di soluzioni di *cloud computing* sono molto diversificati, in costante e significativo aumento e spaziano da sistemi elaborativi virtuali, che sostituiscono o si affiancano ai tradizionali elaboratori ubicati nei locali propri dell'organizzazione, a servizi di supporto allo sviluppo e per l'*hosting* evoluto delle applicazioni, sino a soluzioni *software* rese disponibili in modalità *web* che sono sostitutive delle tradizionali applicazioni installate sui computer di utenti, imprese e di amministrazioni, quali ad esempio applicazioni per l'elaborazione dei testi, per la gestione di agende e calendari, eventualmente condivisi, cartelle per l'archiviazione dei documenti *on-line*, e persino soluzioni esternalizzate di posta elettronica. I dati trasferiti e archiviati per mezzo di questi servizi *web* presso il *service provider* possono essere trattati dagli utenti in remoto attraverso la rete Internet spesso senza la necessità di installare specifici programmi sui propri sistemi e senza l'esigenza di dover effettuare gli aggiornamenti *software* e tutte le altre attività correlate alla manutenzione e alla gestione delle infrastrutture informatiche.

4. I DIVERSI MODELLI DI SERVIZIO

Sul mercato, a seconda delle esigenze dell'utente, sono disponibili varie soluzioni di *cloud computing* erogate secondo modalità che ricadono in linea di massima in tre categorie, dette "modelli di servizio". Comunemente tali modelli di servizio sono riferiti sia a soluzioni di *private cloud* che di *public cloud*, ma vengono qui illustrati in un'ottica maggiormente aderente a quest'ultima tipologia di servizi, che prevede l'utilizzo condiviso da parte di utenti, imprese e soggetti pubblici dei sistemi di *provider* di servizi terzi.

- Nel caso di servizi *IaaS* (*Cloud Infrastructure as a Service* - infrastruttura *cloud* resa disponibile come servizio), il fornitore noleggia un'infrastruttura tecnologica, cioè *server* virtuali remoti che l'utente finale può utilizzare con tecniche e modalità che ne rendono semplice, efficace e produttiva la sostituzione

o l'affiancamento ai sistemi già presenti nei locali dell'azienda. Tali fornitori sono in genere operatori di mercato specializzati che realmente dispongono di un'infrastruttura fisica, complessa e spesso distribuita in aree geografiche diverse.

• Negli *SaaS* (*Cloud Software as a Service - software* erogato come servizio della *cloud*), il fornitore eroga via *web* una serie di servizi applicativi ponendoli a disposizione degli utenti finali. Tali servizi sono spesso offerti in sostituzione delle tradizionali applicazioni installate localmente dall'utente sui propri sistemi, che è quindi spinto ad "esternalizzare" i suoi dati affidandoli al fornitore. Si pensi, ad esempio, ad applicazioni tipiche per l'ufficio erogate in modalità *web* quali fogli di calcolo, elaborazione dei testi, applicazioni per il protocollo informatico, la rubrica dei contatti e i calendari condivisi, ma anche alle moderne offerte di posta elettronica *cloud*.

• Infine, nei *PaaS* (*Cloud platform as a service* - piattaforme *software* fornite via *web* come servizio), il fornitore offre soluzioni per lo sviluppo e l'*hosting* evoluto di applicazioni. In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie, allo scopo di assolvere a esigenze interne oppure per fornire a loro volta servizi a terzi. Anche nel caso dei *PaaS* il servizio erogato dal fornitore elimina la necessità per il fruitore di doversi dotare internamente di strumenti *hardware* o *software* specifici o aggiuntivi.

5. INNOVARE, GOVERNANDO I RISCHI

L'utilizzo di servizi di *cloud computing* è un fenomeno in forte ascesa e determina un cambio di mentalità nelle modalità di utilizzo della rete Internet che, da strumento di condivisione documentale, diviene la porta di accesso alle risorse elaborative e di stoccaggio di fornitori di servizi remoti.

Tale tipologia di servizi comporta la migrazione di dati dai sistemi locali sotto il diretto controllo dell'utente ai sistemi remoti del fornitore, che assume un ruolo

centrale in ordine alla sicurezza dei dati e, quindi, all'adozione delle misure necessarie a garantirla. Tuttavia, è bene evidenziare come l'adozione di servizi esternalizzati non esime le imprese e le amministrazioni pubbliche che se ne avvalgono per la gestione del proprio patrimonio informativo dalle responsabilità che vengono loro attribuite, in particolare, dalla disciplina in materia di protezione dei dati personali.

I trattamenti di dati personali richiedono, infatti, sempre un'attenta ponderazione dei rischi legati alla sicurezza e alla fruibilità delle informazioni, indipendentemente dalle modalità di trattatamento. Pertanto, vanno tenute in debito conto le particolari caratteristiche delle nuove tecnologie, allo scopo di governare i potenziali pericoli che possono derivare da utilizzi scarsamente consapevoli e da modelli innovativi adottati con metodi, prassi e processi non ancora sufficientemente consolidati e in grado di mitigare le eventuali criticità. È quindi opportuno, anche nel caso del *cloud computing*, razionalizzarne le peculiarità al fine di individuare i potenziali rischi insiti in tali servizi e quindi poter adottare efficaci e specifiche misure di prevenzione.

Nel caso del *cloud computing*, il trasferimento dei dati dai computer locali, nella fisica disponibilità e nel diretto controllo esercitabile dal titolare, verso sistemi remoti di proprietà di un terzo fornitore del servizio, presenta, accanto a potenziali utilità, anche i seguenti aspetti che necessitano di specifica attenzione:

- l'utente, affidando i dati ai sistemi di un fornitore remoto, ne perde il controllo diretto ed esclusivo; la riservatezza e la disponibilità delle informazioni allocate sulla nuvola certamente dipendono anche dai meccanismi di sicurezza adottati dal *service provider*;
- il servizio prescelto potrebbe essere il risultato finale di una catena di trasformazione di servizi acquisiti presso altri *service provider*, diversi dal fornitore con cui l'utente stipula il contratto di servizio; l'utente a fronte di filiere di responsabilità complesse potrebbe non sempre essere messo in grado di sapere chi, dei vari gestori dei servizi intermedi, può accedere a determinati dati;

• il servizio virtuale, in assenza di adeguate garanzie in merito alla qualità della connettività di rete, potrebbe occasionalmente risultare degradato in presenza di elevati picchi di traffico o addirittura indisponibile laddove si verifichino eventi anomali quali, ad esempio, guasti, impedendo l'accessibilità temporanea ai dati in esso conservati;

• le *cloud* sono sistemi e infrastrutture condivise basate sul concetto di risorse noleggiate a un'utenza multipla e mutevole; i fornitori, infatti, custodiscono dati di singoli e di organizzazioni diverse che potrebbero avere interessi ed esigenze differenti o persino obiettivi contrastanti e in concorrenza;

• la conservazione dei dati in luoghi geografici differenti ha riflessi immediati sia sulla normativa applicabile in caso di contenzioso tra l'utente e il fornitore, sia in relazione alle disposizioni nazionali che disciplinano il trattamento, l'archiviazione e la sicurezza dei dati;

• l'adozione da parte del fornitore del servizio di tecnologie proprie può, in taluni casi, rendere complessa per l'utente la transizione di dati e documenti da un sistema *cloud* ad un altro o lo scambio di informazioni con soggetti che utilizzino servizi *cloud* di fornitori differenti, ponendone quindi a rischio la portabilità o l'interoperabilità dei dati.

Il fornitore, in base alla tipologia dei servizi offerti, assume la responsabilità di preservare la riservatezza, l'integrità o la disponibilità dei dati; pertanto, l'utente al momento della stipula dei contratti di servizio dovrà tenere in debito conto gli accorgimenti previsti per garantire il corretto trattamento dei dati immessi nella *cloud*.

Prima di adottare un sistema basato nel *cloud computing* è necessario, quindi, valutare attentamente il rapporto tra rischi e benefici derivante dall'utilizzo del predetto servizio virtuale, minimizzando i primi attraverso una attenta verifica dell'affidabilità del fornitore di servizi al quale ci si intende affidare.

6. INDICAZIONI PER L'UTILIZZO CONSAPEVOLE DEI SERVIZI *CLOUD*

• *Ponderare prioritariamente rischi e benefici dei servizi offerti*

Prima di optare per l'adozione di servizi di *cloud computing*, è opportuno che l'utente verifichi la quantità e la tipologia di dati che intende esternalizzare (es. dati personali identificativi o meno, dati sensibili oppure particolarmente delicati come quelli genetici o biometrici, dati critici per la propria attività come ad esempio progetti riservati). E' necessario innanzitutto valutare gli eventuali rischi e le possibili conseguenze derivanti da tale scelta sotto il profilo della riservatezza e della loro rilevanza nel normale svolgimento della propria attività. Tale analisi valutativa dovrà evidenziare l'opportunità o meno di ricorrere a servizi *cloud* (limitandone l'uso ad esempio a determinati tipi di dati), nonché l'impatto sull'utente in termini economici e organizzativi, l'indisponibilità, pur se parziale o per periodi limitati, dei dati esternalizzati o, peggio, la loro perdita o cancellazione.

• *Effettuare una verifica in ordine all'affidabilità del fornitore*

Gli utenti dovrebbero ragionevolmente accertare l'affidabilità del fornitore prima di migrare sui sistemi virtuali i propri dati più importanti, tenendo in considerazione le proprie esigenze istituzionali o imprenditoriali, la quantità e la tipologia delle informazioni che intendono allocare nella *cloud*, i rischi e le misure di sicurezza. In funzione della tipologia di servizio che necessitano, oltre che della criticità dei dati, è opportuno che valutino la stabilità societaria del fornitore, le referenze, le garanzi offerte in ordine alla confidenzialità dei dati e alle misure adottate per garantire la continuità operativa a fronte di eventuali e imprevisti malfunzionamenti. Gli utenti dovrebbero valutare, inoltre, le caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità. Ulteriori criteri in base ai quali è possibile valutare l'affidabilità di un fornitore emergono dall'impiego di personale qualificato, dall'adeguatezza delle infrastrutture informatiche e di comunicazione, dalla disponibilità ad assumersi responsabilità, esplicitamente previste dal contratto di servizio, derivanti da

eventuali falle nel sistema di sicurezza o a seguito di interruzioni di servizio.

• *Privilegiare i servizi che favoriscono la portabilità dei dati*

E' consigliabile ricorrere a servizi di *cloud computing* nelle modalità SaaS, PaaS o IaaS in un'ottica lungimirante, vale a dire privilegiando servizi basati su formati e standard aperti, che facilitino la transizione da un sistema *cloud* ad un altro, anche se gestiti da fornitori diversi. Ciò al fine di scongiurare il rischio che eventuali modifiche unilaterali dei contratti di servizio da parte di uno qualunque degli operatori che intervengono nella catena di fornitura si traducano in condizioni peggiorative vincolanti o, comunque, per facilitare eventuali successivi passaggi da un fornitore all'altro.

• *Assicurarsi la disponibilità dei dati in caso di necessità*

Nell'utilizzo dei servizi di *cloud computing*, in assenza di stringenti vincoli sulla qualità formalizzati attraverso il contratto con il fornitore, si raccomanda di mantenere una copia di quei dati (anche se non personali) dalla cui perdita o indisponibilità potrebbero conseguire danni economici, per l'immagine o in generale relativi alla missione e alle finalità perseguite dall'utente. Ciò specie quando ci si affidi a servizi gratuiti o a basso costo quali, ad esempio, a servizi di *hard-disk* remoto, *mail*, soluzione per la conservazione documentale e così via, che potrebbero non presentare adeguate garanzie di disponibilità e prestazioni tipiche, invece, dei servizi professionali. Certamente, nel caso in cui i dati trattati non siano i propri, come avviene per aziende e pubbliche amministrazioni che raccolgono e detengono informazioni di terzi, l'adozione di servizi che non offrono adeguate garanzie di riservatezza e di continuità operativa può avere rilevanti ripercussioni nel patrimonio informativo dei soggetti cui i dati si riferiscono. In tal senso, il titolare del trattamento dei dati a fronte del contenimento di costi dovrà comunque provvedere al salvataggio (*backup*) dei dati allocati nella *cloud*, ad esempio creandone una copia locale (eventualmente sotto forma di archivio compresso), allo scopo

di gestire gli eventuali rischi insiti nell'acquisizione di servizi che, pur con i vantaggi dell'economicità, potrebbero tuttavia non offrire sufficienti garanzie di affidabilità e di disponibilità.

• *Selezionare i dati da inserire nella cloud*

Alcune informazioni che si intende inserire sui sistemi del fornitore di servizio, per loro intrinseca natura, quali ad esempio i dati sanitari, genetici, reddituali, biometrici o quelli coperti da segreto industriale, possono esigere particolari misure di sicurezza. In tali casi, poiché dal relativo inserimento nella *cloud* consegue comunque una attenuazione, seppur parziale, della capacità di controllo esercitabile dall'utente, ed una esposizione di tali informazioni a rischi non sempre prevedibili di potenziale perdita o di accesso non consentito, l'utente medesimo dovrebbe valutare con responsabile attenzione se ricorrere al servizio di *cloud computing* oppure mantenere *in house* il trattamento di tali tipi di dati.

• *Non perdere di vista i dati*

E' sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto anche verificando se i dati rimarranno nella disponibilità fisica dell'operatore proponente, oppure se questi svolga un ruolo di intermediario, ovvero offra un servizio progettato sulla base delle tecnologie messe a disposizione da un operatore terzo. Si pensi ad esempio a un applicativo in modalità *cloud* nel quale il fornitore del servizio finale (*Software as a Service*) offerto all'utente si avvalga di un servizio di stoccaggio dati acquisito da un terzo. In tal caso, saranno i sistemi fisici di quest'ultimo operatore che concretamente ospiteranno i dati immessi nella *cloud* dall'utente.

• *Informarsi su dove risiederanno, concretamente, i dati*

Sapere in quale Stato risiedono fisicamente i *server* sui quali vengono allocati i dati, è determinate per stabilire la giurisdizione e la legge applicabile nel caso di

controversie tra l'utente e il fornitore del servizio. La presenza fisica dei *server* in uno Stato comporterà per l'autorità giudiziaria nazionale, infatti, la possibilità di dare esecuzione ad ordini di esibizione, di accesso o di sequestro, ove sussistano i presupposti giuridici in base al singolo ordinamento nazionale. Non è, quindi, indifferente per l'utente sapere se i propri dati si trovino in un *server* in Italia, in Europa o in un imprecisato Paese extraeuropeo. In ogni caso, l'utente, prima di inserire i dati nella nuvola informatica, dovrebbe assicurarsi che il trasferimento tra i diversi paesi in cui risiedono le *cloud* avvenga nel rispetto delle cautele previste a livello di Unione europea in materia di protezione dei dati personali, che esigono particolari garanzie in ordine all'adeguatezza del livello di tutela previsto dagli ordinamenti nazionali per tale tipo di informazioni.

• *Attenzione alle clausole contrattuali*

Una corretta e oculata gestione contrattuale può supportare sia l'utente, sia il fornitore nella definizione delle modalità operative e dei parametri di valutazione del servizio, oltre a individuare i parametri di sicurezza necessari per la tipologia di attività gestita. In ogni caso, è importante valutare l'idoneità delle condizioni contrattuali per l'erogazione del servizio di *cloud* con riferimento ad obblighi e responsabilità in caso di perdita, smarrimento dei dati custoditi nella nuvola e di conseguenze in caso di decisione di passaggio ad altro fornitore. Costituiscono elementi da privilegiare la previsione di garanzie di qualità chiare, corredate da penali che pongano a carico del fornitore eventuali inadempienze o le conseguenze di determinati eventi (es. accesso non consentito, perdita dei dati, indisponibilità per malfunzionamenti, ecc.). Si suggerisce, inoltre, di verificare eventuali soggetti terzi delegati alla fornitura di servizi intermedi e che concorrono all'erogazione del servizio finale rivolto all'utente, ovvero la preventiva identificazione dei diversi fornitori successivamente coinvolti nel trattamento. Si raccomanda, infine, di accertare quale sia la quantità di traffico dati prevista dal contratto oltre la quale vengono addebitati oneri economici supplementari.

• *Verificare le politiche di persistenza dei dati legate alla loro conservazione*

In fase di acquisizione del servizio *cloud* è opportuno approfondire le politiche adottate dal fornitore, che si dovrebbero poter evincere dal contratto, relative ai tempi di persistenza dei dati nella nuvola. Da una parte l'utente dovrebbe accertare il termine ultimo, successivo alla scadenza del contratto, oltre il quale il fornitore cancella definitivamente i dati che gli sono stati affidati. Dall'altra, il fornitore dovrà presentare adeguate garanzie, assicurando che i dati non saranno conservati oltre i suddetti termini o comunque al di fuori di quanto esplicitamente stabilito con l'utente stesso. In ogni caso, i dati dovranno essere sempre conservati nel rispetto delle finalità e delle modalità concordate, escludendo duplicazioni e comunicazioni a terzi.

• *Esigere e adottare opportune cautele per tutelare la confidenzialità dei dati*

Nell'ottica di proteggere la confidenzialità dei propri dati, l'utente dovrebbe valutare anche le misure di sicurezza utilizzate dal fornitore per consentire l'allocazione dei dati nella *cloud*. In generale si raccomanda di privilegiare i fornitori che utilizzano a tal fine tecniche di trasmissione sicure, tramite connessioni cifrate (specie quando i dati trattati sono informazioni personali o comunque dati che devono restare riservati), coadiuvate da meccanismi di identificazione dei soggetti autorizzati all'accesso, la cui complessità sia commisurata alla criticità dei dati stessi. Nella maggior parte dei casi risulta adeguato l'utilizzo di semplici meccanismi di identificazione, basati su *username* e *password*, purché le *password* non siano banali e vengano scelte di lunghezza adeguata. Nell'ipotesi in cui il trattamento riguardi particolari tipologie di dati - quali quelli sanitari, genetici, reddituali e biometrici o, più in generale, dati la cui riservatezza possa considerarsi "critica" - si raccomanda oltre all'utilizzo di protocolli sicuri nella fase di trasmissione, anche la conservazione in forma cifrata sui sistemi del fornitore di servizio.

• *Formare adeguatamente il personale*

Il personale preposto al trattamento di dati attraverso i servizi di *cloud computing* dovrebbe essere sottoposto a specifici interventi formativi, che evidenzino adeguatamente

le modalità più idonee per l'acquisizione e l'inserimento dei dati nella *cloud*, la consultazione e in generale l'utilizzo dei nuovi servizi esternalizzati e delle indicazioni sin qui illustrate, allo scopo di mitigare rischi per la protezione dei dati derivanti non solo da eventuali comportamenti sleali o fraudolenti, ma anche causati da errori materiali, leggerezza o negligenza: circostanze queste che potrebbero dare luogo ad accessi illeciti, perdita di dati o, più in generale, trattamenti non consentiti.