CLOUD COMPUTING

PROTEGGERE I DATI
PER NON CADERE DALLE NUVOLE

Mini guida per imprese
e pubblica amministrazione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

COS'È IL CLOUD COMPUTING 4

NUVOLE DIVERSE PER ESIGENZE DIVERSE 8

IL QUADRO GIURIDICO 12

VALUTAZIONE DEI RISCHI, DEI COSTI E DEI BENEFICI 18

IL DECALOGO PER UNA SCELTA CONSAPEVOLE 24

CLOUD COMPUTING

PROTEGGERE I DATI
PER NON CADERE DALLE NUVOLE

Ogni imprenditore, ma anche ogni attento amministratore pubblico, si adopera per offrire, rispettivamente ai propri clienti e ai cittadini, servizi migliori a minor costo. Le tecnologie informatiche, in particolare quelle del cloud computing, garantiscono oggi soluzioni innovative per gestire molteplici attività con efficienza e possibili risparmi. Ma presentano criticità e rischi per la privacy di cui è bene tenere conto. Prima di esternalizzare la gestione di dati e documenti o adottare nuovi modelli organizzativi è necessario porsi alcune domande, scegliendo con cura la soluzione più sicura per le attività istituzionali o per il proprio business. Con questo vademecum, il Garante per la protezione dei dati personali intende offrire alcune indicazioni valide per tutti gli utenti, in particolare imprese e amministrazioni pubbliche. L'obiettivo è quello di far riflettere su alcuni importanti aspetti giuridici, economici e tecnologici in un settore in velocissima espansione e di promuovere un utilizzo corretto delle nuove modalità di erogazione dei servizi informatici.

COS'È IL CLOUD COMPUTING

Con il termine cloud computing, o semplicemente cloud, ci si riferisce a un insieme di tecnologie e di modalità di fruizione di servizi informatici che favoriscono l'utilizzo e l'erogazione di software, la possibilità di conservare e di elaborare grandi quantità di informazioni via Internet.
Il cloud offre, a seconda dei casi, il trasferimento della conservazione o dell'elaborazione dei dati dai computer degli utenti ai sistemi del fornitore.
Il cloud consente, inoltre, di usufruire di servizi complessi senza doversi necessariamente dotare né di computer e altri hardware avanzati, né di personale in grado di programmare o gestire il sistema.

Tutto può essere demandato all'esterno, in *outsourcing*, e a un costo potenzialmente limitato, in quanto le risorse informatiche necessarie per i servizi richiesti possono essere condivise con altri soggetti che hanno le stesse esigenze.

L'AUTOMOBILE "INFORMATICA" E IL CLOUD PER PROFANI

Opzione 1 – tutto in casa: se una persona o una società ha bisogno di un'automobile può progettarla, acquistarne le singole componenti e assemblarle, nonché attrezzare all'interno della propria casa o della propria sede un'officina con personale specializzato per le riparazioni e la manutenzione.

Opzione 2 – intervento esterno: si può decidere di acquistare l'automobile e di portarla in caso di necessità da un meccanico di fiducia, di affittarla, di prenderla in leasing, di chiamare un taxi o noleggiare una vettura con autista. La scelta tra queste opzioni è determinata dal tipo di utilizzo che si vuole fare dell'autoveicolo, dalla frequenza con cui se ne fruisce, dalle prestazioni che eventualmente si desiderano e, comunque, dalle risorse economiche a disposizione.

Con il cloud computing ci troviamo in questa seconda opzione.
Non parliamo di automobili o altri mezzi di trasporto ma di servizi informatici. Le soluzioni offerte dal cloud generalmente possono essere più flessibili, efficienti, adattabili ed economiche di quelle sviluppate *in-house* (in casa propria).
Ma possono comportare il rischio di una potenziale perdita di controllo sui propri dati.

Spesso utilizziamo tecnologie cloud senza neppure saperlo. Alcuni dei più diffusi servizi di posta elettronica o di elaborazione testi sono "sulle nuvole". Anche molte delle funzioni offerte dai cellulari di nuova generazione (i cosiddetti smartphone) sono basate sul cloud: ad esempio quelle che sfruttano la geolocalizzazione consigliandoci i locali o gli esercizi commerciali più vicini, che consentono di ascoltare musica o di accedere a giochi on line, nonché tante altre funzioni e "app"(applicazioni).

NUVOLE DIVERSE PER ESIGENZE DIVERSE

Esistono vari tipi di cloud computing, classificati sia in base all'architettura della "nuvola" e alla gestione interna o esterna del trattamento dati, sia in relazione al modello di servizio offerto al cliente. Ogni tipo di cloud ha le sue caratteristiche peculiari che dovranno essere ben valutate dalle società e dalle pubbliche amministrazioni che intendono servirsi delle "nuvole".

TIPI DI CLOUD

Private Cloud
La "nuvola privata" è una infrastruttura informatica (rete di computer collegati per offrire servizi) 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 esercitare un controllo puntuale. Le "nuvole private" 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 agevolmente in caso di necessità.

Public Cloud
Nel caso della "nuvola pubblica", l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni i propri sistemi attraverso la condivisione e l'erogazione via Internet di applicazioni informatiche, di capacità elaborativa e di "stoccaggio" dati. La fruizione di tali

servizi avviene tramite la rete Internet e implica il trasferimento dei soli dati o anche dell'attività di elaborazione presso i sistemi del fornitore del servizio, il quale assume un ruolo importante in ordine all'efficacia delle misure adottate per garantire la protezione delle informazioni che gli sono state affidate. Con il cloud pubblico l'utente insieme ai dati, infatti, cede una parte importante del controllo esercitabile su di essi.

Altre "nuvole"
Esistono altri tipi di nuvole con caratteristiche miste, quali i cloud ibridi (*hybrid cloud*) - caratterizzati da soluzioni che prevedono l'utilizzo di servizi erogati da infrastrutture private accanto a servizi acquisiti da cloud pubblici - e i cloud di gruppo (*community cloud*), in cui l'infrastruttura è condivisa da diverse organizzazioni a beneficio di una specifica comunità di utenti.

TRE MODELLI DI SERVIZI CLOUD

Cloud Infrastructure as a Service - IaaS
(infrastruttura cloud resa disponibile come servizio)
Il fornitore del servizio cloud offre, secondo un modello "a consumo", gli strumenti hardware e software di base

(spazi di memoria, sistemi operativi, programmi di virtualizzazione...), cioè server virtuali remoti che l'utente finale può utilizzare in sostituzione o in affiancamento ai sistemi già presenti nei locali dell'azienda o dell'amministrazione. Tali fornitori sono in genere operatori di mercato specializzati, che dispongono di un'infrastruttura tecnologica, complessa e spesso distribuita in aree geografiche diverse.

Cloud Software as a Service - SaaS
(software erogato come servizio del cloud)
Il fornitore eroga via Internet una serie di servizi applicativi ponendoli a disposizione degli utenti finali.
Si pensi, ad esempio, ad applicazioni comunemente usate negli uffici erogate in modalità web quali 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 i calendari condivisi, ma anche ai più avanzati servizi di posta elettronica.

Cloud Platform as a Service - PaaS
(piattaforme software fornite via Internet come servizio)
Il fornitore offre soluzioni evolute di sviluppo software che rispondono alle specifiche esigenze del cliente.
In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie (ad esempio applicativi per la gestione finanziaria, della contabilità o della logistica), 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 limita la necessità per il fruitore di doversi dotare internamente di strumenti hardware o software specifici o aggiuntivi.

IL QUADRO GIURIDICO

LA SFIDA INTERNAZIONALE

La tecnologia cloud procede molto più velocemente dell'attività del legislatore, non solo in Italia ma in tutto il mondo. Manca ancora un quadro normativo aggiornato – in tema di privacy, ma anche in ambito civile e penale - che tenga conto di tutte le novità introdotte dal cloud computing e sia in grado di offrire adeguate tutele nei riguardi delle fattispecie giuridiche connesse all'adozione di servizi distribuiti di elaborazione e di conservazione dati. Basti pensare, ad esempio, che la normativa europea sulla protezione dei dati risale al 1995.
Alcune utili novità per il settore delle telecomunicazioni, che avranno un indubbio impatto anche sul cloud, sono state introdotte dal cosiddetto "pacchetto Telecom": in particolare dalla direttiva 136/2009 - attualmente in corso di recepimento da parte degli Stati membri dell'Ue – che modifica la direttiva sulla privacy nelle comunicazioni elettroniche del 2002. Fra le misure che entreranno in vigore con il nuovo quadro giuridico è previsto anche l'obbligo per le società telefoniche e gli Internet provider di notificare alle competenti Autorità nazionali e, in determinati casi, agli utenti, tutte le violazioni di sicurezza che comportino la distruzione, la perdita o la diffusione indebita di dati personali trattati nell'ambito della fornitura del servizio.
Un ulteriore importante cambiamento per tutto il settore delle comunicazioni elettroniche, e del cloud computing in particolare, dovrebbe avvenire entro il 2014, con l'approvazione del nuovo Regolamento generale sulla protezione dei dati (Com 2012 11 def) proposto

dalla Commissione Europea.
Il nuovo Regolamento introdurrà identiche regole in Europa e nei confronti di Stati terzi (riscrivendo quindi anche il Codice della privacy italiano), e in questo senso dovrebbe contribuire a rendere meno complesso e rischioso l'utilizzo di servizi cloud. Una delle importanti innovazioni di questa riforma riguarderà l'estensione dell'obbligo di notifica delle violazioni di sicurezza che riguardino dati personali a tutti i titolari del trattamento dati come, ad esempio, banche, assicurazioni, Asl, enti locali. Quando previsto, le persone interessate saranno quindi informate senza ritardo della perdita o del furto dei loro dati.

NORMATIVA PRIVACY NELLE NUVOLE – SPUNTI DI RIFLESSIONE

In attesa di una normativa nazionale e internazionale aggiornata e uniforme, che permetta di governare il fenomeno senza rischiare di penalizzare l'innovazione e le potenzialità di sviluppo delle "nuvole" informatiche, è necessario che le imprese e la pubblica amministrazione, incluse tra l'altro le cosiddette "centrali di committenza" (soggetti che effettuano acquisti per una pluralità di pubbliche amministrazioni), prestino particolare attenzione ai rischi connessi all'adozione dei servizi di cloud computing, anche in relazione agli aspetti di protezione dei dati personali.

Il titolare e il responsabile del trattamento
La pubblica amministrazione o l'azienda, "titolare del trattamento" dei dati personali, che trasferisce del tutto o in parte il trattamento sulle "nuvole", deve procedere a designare il fornitore dei servizi cloud "responsabile del trattamento".

Questo significa che il cliente dovrà sempre prestare molta attenzione a come saranno utilizzati e conservati i dati personali caricati sulla "nuvola": in caso di violazioni commesse dal fornitore, anche il titolare sarà chiamato a rispondere dell'eventuale illecito.
Il cliente di ridotte dimensioni, come una piccola impresa o un ente locale, potrebbe tuttavia incontrare difficoltà nel contrattare adeguate condizioni per la gestione dei dati spostati "sulla nuvola". Anche in questo caso, non sarà però sufficiente, per giustificare una eventuale violazione, affermare di non avere avuto possibilità di negoziare clausole contrattuali o modalità di controllo più stringenti. Il cliente di servizi cloud, infatti, può sempre rivolgersi ad altri fornitori che offrono maggiori garanzie, in particolare per il rispetto della normativa sulla protezione dei dati. Il Codice della privacy prevede,

tra l'altro, che il titolare eserciti un potere di controllo nei confronti del responsabile del trattamento (in questo caso il cloud provider), verificando la corretta esecuzione delle istruzioni impartite in relazione ai dati personali trattati.

Trasferimento dei dati fuori dell'Unione Europea

Il Codice della privacy definisce regole precise per il trasferimento dei dati personali fuori dall'Unione europea e vieta, in linea di principio, il trasferimento "anche temporaneo" di dati personali verso uno Stato

extraeuropeo, qualora l'ordinamento del Paese di destinazione o di transito dei dati non assicuri un adeguato livello di tutela. Questa evenienza può verificarsi frequentemente nel caso in cui si decida di usufruire di servizi di *public cloud* invece che di modalità private o ibride. Per le sue valutazioni il titolare del trattamento (in genere chi acquista servizi cloud) dovrà quindi tenere in debito conto anche il luogo dove vengono conservati i dati e quali sono i trattamenti previsti all'estero.
Il trasferimento di dati verso gli Stati Uniti, ad esempio, può essere facilitato nel caso in cui il cloud provider aderisca a programmi di protezione dati come il cosiddetto *Safe Harbor* (letteralmente "porto sicuro"), un accordo bilaterale Ue-Usa che definisce regole sicure e condivise per il trasferimento dei dati personali effettuato verso aziende presenti sul territorio americano.

Le limitazioni per il trasferimento dati all'estero incidono anche sugli spostamenti "infragruppo" di una multinazionale.
In questo caso, la presenza di forti "norme vincolanti d'impresa" (*binding corporate rules*) a tutela dei dati personali può consentire l'eventuale trasferimento dei dati nel rispetto della privacy degli interessati.

Sicurezza dei dati
Il titolare del trattamento deve assicurarsi che siano adottate misure

tecniche e organizzative volte a ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, di modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole. Il cliente dovrebbe, ad esempio, accertarsi che i dati siano sempre "disponibili" (che si possa cioè sempre accedere ai dati) e "riservati" (che l'accesso cioè sia consentito solo a chi ne ha diritto). Per garantire che i dati siano al sicuro, non sono importanti solo le modalità con cui sono conservati, ma anche quelle con cui sono trasmessi (ad esempio utilizzando tecniche di cifratura).

I diritti dell'interessato

I soggetti pubblici e le imprese che decidono di avvalersi di servizi cloud per gestire i dati personali dei loro utenti o clienti non devono dimenticare che il Codice della privacy attribuisce agli interessati (le persone a cui si riferiscono i dati) precisi diritti. Ad esempio, l'interessato ha diritto di conoscere quali siano i dati che lo riguardano in possesso dell'amministrazione pubblica o dell'impresa, per quale motivo siano stati raccolti e come siano elaborati. Può richiedere una copia intelligibile dei dati personali che lo riguardano, il loro aggiornamento, la rettifica o l'integrazione. In caso di violazione di legge, può esigere anche il blocco, la cancellazione o la trasformazione in forma anonima di queste informazioni. Il cliente del servizio cloud, in qualità di titolare del trattamento dati, per soddisfare queste richieste, deve poter mantenere un adeguato controllo non solo sulle attività del fornitore, ma anche su quelle degli eventuali sub fornitori dei quali il cloud provider potrebbe avvalersi.

VALUTAZIONE DEI RISCHI, DEI COSTI E DEI BENEFICI

È opportuno scegliere bene il tipo di cloud e il modello di servizio più adatto alle proprie esigenze. In particolare se si decide di adottare il *public cloud*, dove quasi tutto il processo viene esternalizzato e i "nostri" dati più preziosi sono dislocati "lontano" dal nostro controllo diretto. Il concetto di cloud può apparire evanescente, "virtuale".
In realtà, con le sue tecnologie si possono gestire servizi estremamente concreti, quali la distribuzione dei prodotti di un'azienda, i servizi dell'anagrafe di un Comune, le prenotazioni e le analisi mediche, il conto bancario on line e tanto altro. Nessuno lascerebbe in deposito il proprio portafoglio con i documenti e lo stipendio alla prima persona incontrata al mercato. Né affiderebbe il proprio libro mastro o i contratti stipulati con clienti e fornitori a un commercialista sconosciuto che gli promette di risparmiare, senza prima essersi accertato su come saranno conservati o utilizzati documenti così preziosi. La voce "risparmio" non deve quindi essere l'unico fattore di scelta.
I grandi fornitori globali di cloud computing si contano sulle dita di una mano. Quasi tutte le altre società che offrono servizi e infrastrutture tra le "nuvole" si avvalgono infatti delle aziende leader mondiali. Questa situazione riduce di molto la capacità negoziale di una singola impresa o di una piccola amministrazione pubblica, rendendo difficile trasformare la flessibilità tecnologica in flessibilità contrattuale.
In questi casi la scelta di consorziarsi con altri soggetti pubblici o imprese che hanno le medesime esigenze (ad esempio tramite le associazioni di categoria) potrebbe garantire una capacità contrattuale maggiore.
Prima di optare per un certo tipo di "nuvola", è comunque opportuno che l'utente verifichi la quantità e la tipologia

di dati che intende esternalizzare (ad esempio dati personali, in particolare quelli sensibili, oppure dati critici per la propria attività, come progetti riservati o coperti da brevetto o segreto industriale), valutando gli eventuali rischi e le possibili conseguenze derivanti da tale scelta. È vero che il cliente spesso non ha capacità di negoziare una riformulazione dei "*term of use*" proposti da chi offre i servizi: può però scegliere tra differenti provider. Anche i fornitori cloud, comunque, potrebbero trarre nuove opportunità dalla definizione di clausole "pro-privacy" o da una eventuale preventiva certificazione indipendente sul rispetto della normativa europea sulla protezione dei dati personali per i servizi da loro offerti. La risposta ad alcune domande può aiutare a sviluppare una corretta analisi dell'impatto economico e organizzativo di queste tecnologie all'interno di un'impresa o di una pubblica amministrazione.

SICUREZZA

Quali sono le misure di sicurezza adottate dal fornitore per proteggere i dati? Il fornitore di servizi cloud spesso dispone di sistemi di protezione contro virus, attacchi hacker o altri pericoli informatici più efficaci rispetto a quelli che potrebbe permettersi il singolo utente. È comunque necessario informarsi bene su quali siano le misure adottate dal cloud provider. Prima di scegliere il partner cloud il cliente deve sempre considerare che, affidandosi a un fornitore remoto, può perdere il controllo diretto ed esclusivo sui propri dati.

RUOLI E RESPONSABILITÀ

Chi è il reale fornitore del servizio che si sta acquisendo? Si tratta di una singola società o di un consorzio di imprese? 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 essere messo in grado di sapere chi, tra i vari gestori dei servizi intermedi, può accedere a determinati dati.

DISPONIBILITÀ DEL SERVIZIO E PIANO DI EMERGENZA

In caso di problemi al collegamento Internet, è comunque possibile continuare a usufruire dei servizi senza l'accesso al cloud? In quanto tempo può essere ripristinato il sistema? Esistono piani di emergenza per i servizi essenziali? Il servizio virtuale, in assenza di adeguate garanzie in merito alla qualità della connettività di rete, potrebbe occasionalmente risultare degradato in presenza di attacchi informatici, di elevati picchi di traffico o addirittura

indisponibile laddove si verifichino eventi anomali o guasti che impediscano l'accessibilità temporanea ai dati. È quindi necessario valutare bene le conseguenze sulla propria società o ente dell'eventuale interruzione, più o meno prolungata, del servizio, considerare i costi diretti e indiretti dell'inaccessibilità ai dati, e definire in anticipo con il fornitore cloud un eventuale piano di emergenza.

RECUPERO DEI DATI

È possibile che i dati sul cloud possano essere persi o distrutti? Calamità naturali o attacchi informatici potrebbero compromettere il funzionamento di alcuni data center. È particolarmente importante individuare possibili procedure di recupero dei dati

e quantificare l'impatto economico e organizzativo dell'eventuale perdita o cancellazione di dati presenti solo sul cloud.

CONFIDENZIALITÀ

Esistono garanzie di riservatezza per i nostri dati nel caso in cui un concorrente condivida gli stessi servizi cloud?
I fornitori custodiscono dati di singoli e di organizzazioni che potrebbero avere interessi ed esigenze differenti o persino obiettivi contrastanti e in concorrenza. È quindi opportuno valutare le garanzie offerte a tutela della confidenzialità delle informazioni trasferite sul cloud.

COLLOCAZIONE DEI SERVER

In quale Stato sono conservati i dati caricati sulla "nuvola"? È possibile scegliere di usufruire di server collocati solo in territorio nazionale o in Paesi dell'Unione europea? L'identificazione del luogo in cui i dati sono conservati o elaborati ha riflessi immediati sia sulla normativa applicabile in caso di contenzioso tra il cliente e il fornitore, sia in relazione alle disposizioni nazionali che disciplinano il trattamento, l'archiviazione e la sicurezza dei dati.
La conoscenza di questi elementi garantirà un rapporto più trasparente tra il cliente e il fornitore di cloud computing. È poi necessario non dimenticare che la normativa sulla privacy, al fine di tutelare le persone interessate, prevede che i dati possano essere "esportati" in Paesi fuori dall'Unione europea solo in precisi casi e quando sia offerta una protezione adeguata rispetto a quella prevista dalla legislazione comunitaria. Un servizio cloud potrebbe quindi celare dei costi extra imprevisti, determinati dalla ridotta capacità di controllo sui propri dati o da più probabili contenziosi legali nazionali e internazionali.

MIGRAZIONE

La tecnologia utilizzata dal fornitore di cloud è di tipo "proprietario"? I dati possono essere esportati facilmente? L'adozione da parte del fornitore del servizio di tecnologie proprie può, in taluni casi, rendere complessa per l'utente la migrazione 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, ponendo quindi a rischio la portabilità o l'interoperabilità dei dati. Questa evenienza potrebbe dare luogo a politiche commerciali poco trasparenti. In un primo momento, il fornitore potrebbe ad esempio presentare al cliente un'offerta di servizi cloud economicamente vantaggiosa e con adeguate garanzie a protezione dei dati. In un secondo momento, una volta acquisito il cliente, potrebbe invece cambiare le condizioni del contratto a proprio vantaggio con la certezza che il cliente - considerata l'impossibilità pratica di trasferire agevolmente i dati presso un altro fornitore e di recedere dal servizio - non potrà far altro che accettarle.

ASSICURAZIONE SUL DANNO

Nel caso in cui si accerti una violazione o la perdita dei dati, il fornitore garantisce un pronto risarcimento del danno? Le attuali incertezze normative possono rendere difficile e oneroso riuscire a ottenere un adeguato risarcimento per i danni subiti in seguito a violazioni, a perdita di dati, a interruzione anche temporanea del servizio cloud.
La presenza di un'assicurazione o di procedure semplificate per la risoluzione di controversie, anche internazionali, può sicuramente essere un valore aggiunto per utenti di piccole dimensioni.

IL DECALOGO PER UNA SCELTA CONSAPEVOLE

1

EFFETTUARE UNA VERIFICA SULL'AFFIDABILITÀ DEL FORNITORE

Gli utenti dovrebbero accertare l'esperienza, la capacità e l'affidabilità del fornitore prima di trasferire sui sistemi cloud i propri dati più preziosi, tenendo in considerazione le proprie esigenze istituzionali o imprenditoriali, la quantità e la tipologia delle informazioni che intendono allocare, i rischi e le misure di sicurezza adottate. Anche in funzione della tipologia di servizio desiderato, oltre che della criticità dei dati, è opportuno che gli utenti valutino: la struttura societaria del fornitore, le referenze, le garanzie di legge offerte in ordine alla confidenzialità dei dati e alle misure adottate per assicurare 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. Sarà utile considerare anche l'impiego da parte del fornitore di personale qualificato, l'adeguatezza delle sue infrastrutture informatiche e di comunicazione, la disponibilità ad assumersi una responsabilità risarcitoria (che dovrebbe essere esplicitamente prevista dal contratto di servizio) in caso di eventuali falle nel sistema di sicurezza o di interruzioni del servizio.

2

PRIVILEGIARE I SERVIZI CHE FAVORISCONO LA PORTABILITÀ DEI DATI

È consigliabile ricorrere a servizi di cloud computing privilegiando quelli basati su formati e standard aperti, che facilitino la transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi.

La portabilità dei dati consente di recedere dal servizio senza incorrere in spese e disagi difficilmente prevedibili. Tale opzione limita anche il rischio che i fornitori, sfruttando la loro posizione di forza negoziale, adottino eventuali modifiche unilaterali e peggiorative dei contratti di servizio cloud instaurati con il cliente.

3

ASSICURARSI LA DISPONIBILITÀ DEI DATI IN CASO DI NECESSITÀ

È opportuno chiedere che nel contratto con il fornitore siano ben specificate adeguate garanzie sulla disponibilità e sulle prestazioni dei servizi cloud. L'adozione di servizi che non offrono adeguate garanzie di riservatezza e di continuità operativa può comportare rilevanti ripercussioni non solo sul cliente del servizio cloud, ma anche sui soggetti a cui si riferiscono i dati personali trattati, come avviene per le pubbliche amministrazioni e per le società che offrono servizi a terzi. In tal senso, a fronte del contenimento dei costi, il titolare del trattamento (in genere chi acquista servizi cloud) dovrà comunque prevedere la possibilità di conservare una copia dei dati allocati sul cloud, in particolare di quelli la cui perdita o indisponibilità potrebbe causare gravissimi danni, non solo economici o di immagine: si pensi a dati particolarmente delicati come quelli di tipo sanitario o giudiziario, o di carattere fiscale e patrimoniale.

4

SELEZIONARE I DATI DA INSERIRE NELLA NUVOLA

Alcune informazioni, come quelle coperte da segreto industriale e tutti i dati sensibili (ad esempio quelli relativi alla salute, all'etnia, alle opinioni politiche o alle iscrizioni a sindacati), richiedono, per loro intrinseca natura, particolari misure di sicurezza.

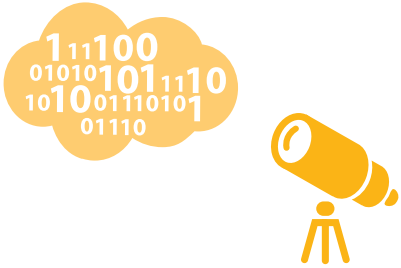
In tali casi, poiché dall'inserimento dei dati nel cloud consegue comunque una inferiore capacità di controllo diretto da parte dell'utente e un'esposizione a rischi non sempre prevedibili di perdita o di accesso abusivo, è bene valutare con responsabile attenzione se ricorrere ai servizi di cloud computing (in particolare di tipo "pubblico"), oppure se utilizzare altre forme di *outsourcing*, ovvero mantenere "in sede" il trattamento di tali dati.

5

NON PERDERE DI VISTA I DATI

È sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto, anche verificando se i dati rimarranno nella disponibilità fisica dell'operatore con cui è stato stipulato il contratto oppure se questi svolga un ruolo di intermediario, ovvero offra un servizio basato sulle 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 di elaborazione dati si avvalga di un servizio di "stoccaggio" acquisito da un terzo. In tal caso, saranno i sistemi fisici di quest'ultimo operatore che concretamente ospiteranno i dati immessi nel cloud dall'utente. Per valutare la qualità del cloud è quindi necessario informarsi sulle prestazioni offerte da tutti i soggetti coinvolti nella fornitura del servizio.

6

INFORMARSI SU DOVE RISIEDERANNO, CONCRETAMENTE, I DATI

È importante per l'utente sapere se i propri dati vengono trasferiti ed elaborati da server in Italia, in Europa o in un Paese extraeuropeo. Tale informazione può essere determinante per stabilire la giurisdizione e la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio, ma soprattutto per verificare il livello di protezione assicurato ai dati.
Il trasferimento di dati in Paesi che non offrono adeguate garanzie di sicurezza e confidenzialità potrebbe comportare un illecito trattamento dei dati personali, oltre a eventuali danni irreparabili per le attività istituzionali dei soggetti pubblici o per il business delle imprese.
In ogni caso, l'utente, prima di caricare i dati "sulla nuvola" e di consentire il loro eventuale trasferimento in Paesi fuori dall'Unione europea, deve accertarsi che questo spostamento avvenga nel rispetto delle garanzie previste dalla normativa italiana e comunitaria in tema di protezione dei dati personali.
Se l'azienda, ad esempio, è statunitense è bene verificare che abbia aderito all'accordo *Safe Harbor* che definisce regole condivise con le istituzioni europee per il trattamento dei dati personali.
Così come è utile controllare che

le aziende al di fuori dell'Ue coinvolte nel cloud abbiano sottoposto le proprie procedure di sicurezza e di trattamento dei dati a specifici percorsi di certificazione, come quelli regolati dagli standard ISO per la gestione della sicurezza. Oppure se nei contratti di *outsourcing* proposti al cliente siano state inserite le specifiche "clausole contrattuali tipo" approvate dalla Commissione europea per i trasferimenti di dati personali verso Paesi terzi.

7

ATTENZIONE ALLE CLAUSOLE CONTRATTUALI

È importante valutare l'idoneità delle condizioni contrattuali per l'erogazione del servizio di cloud con particolare riferimento agli obblighi e alle responsabilità in caso di perdita e di illecita diffusione dei dati custoditi nella "nuvola", nonché alle eventuali modalità per il recesso dal servizio e il passaggio ad altro fornitore.
Un elemento da privilegiare è senz'altro la previsione di garanzie di qualità chiare, corredate da penali, che pongano a carico del fornitore le eventuali inadempienze o le conseguenze di determinati eventi (ad es. accesso non consentito, perdita dei dati, indisponibilità per malfunzionamenti ecc.).
Si suggerisce di verificare anche l'eventuale partecipazione di ulteriori soggetti che concorrano come subfornitori all'erogazione del servizio cloud e all'eventuale trattamento dei dati.

8

VERIFICARE TEMPI E MODALITÀ DI CONSERVAZIONE DEI DATI

In fase di acquisizione del servizio cloud è opportuno approfondire e prevedere nel contratto le politiche adottate dal fornitore riguardo ai tempi

di conservazione dei dati nella nuvola. Ove non sia già prevista per legge l'immediata cancellazione dei dati del titolare allo scadere del contratto cloud, è necessario accertare il termine ultimo oltre il quale il fornitore (responsabile del trattamento) debba cancellare definitivamente i dati a lui affidati. Il fornitore dovrà quindi assicurare 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 solo nel rispetto delle finalità e delle modalità concordate.

9

ESIGERE ADEGUATE MISURE DI SICUREZZA

Nell'ottica di proteggere la confidenzialità dei dati, occorre valutare con attenzione anche le misure di sicurezza utilizzate dal fornitore del servizio cloud. In generale si raccomanda di privilegiare i fornitori che utilizzino modalità di archiviazione e trasmissione sicure, mediante tecniche crittografiche (specialmente quando i dati trattati sono particolarmente delicati), accompagnate da robusti meccanismi di identificazione dei soggetti autorizzati all'accesso.

10

FORMARE ADEGUATAMENTE IL PERSONALE

Il personale, sia quello del cliente che quello del fornitore, incaricato del trattamento dei dati mediante servizi di cloud computing dovrebbe essere

appositamente formato, al fine di limitare rischi di accesso illecito, di perdita di dati o, più in generale, di trattamento non consentito. L'attività di formazione dovrebbe riguardare sia gli elementi tecnici che consentono una scelta consapevole delle tecnologie cloud adottate, sia le fasi operative del trattamento, come l'inserimento dei dati sulla "nuvola" e la loro elaborazione. La protezione dei dati può infatti essere messa a repentaglio non solo da eventuali comportamenti sleali o fraudolenti, ma anche da errori materiali, leggerezza o negligenza del personale.

UNA PRECAUZIONE EXTRA PER GLI UTENTI PRIVATI

Le disposizioni previste dal Codice della privacy non si applicano a singole persone che trattano i dati per scopi personali, senza diffonderli magari su Internet e senza effettuare comunicazioni sistematiche di tali dati a più individui. È comunque opportuno ricordare che anche le cosiddette "persone fisiche" sono tenute a conservare con cura i dati affinché la loro eventuale perdita non possa causare danni ad altre persone. L'adozione di nuove tecnologie per la mobilità, come smartphone e tablet, dotati di grandi quantità di memoria, spesso connessi a servizi cloud non protetti che consentono di sfruttare lo stesso strumento per attività private e professionali, ha però aumentato il rischio di perdita di controllo dei dati personali. Si consiglia quindi di conservare con cura gli strumenti tecnologici utilizzati per scopi personali, e di adottare tutte le cautele al fine di impedire accessi anche accidentali, da parte di terzi, ai dati personali.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771
fax 06 696773785

VERTIGO DESIGN

Per informazioni presso l'Autorità:
Ufficio per le relazioni con il pubblico
Lunedì - Venerdì ore 10.00 - 13.00
tel. 06 696772917/9
e-mail: urp@garanteprivacy.it
pec: urp@pec.gpdp.it

**A cura del Servizio relazioni
con i mezzi di informazione**

www.garanteprivacy.it

Stampa: IAG Mengarelli - maggio 2012