

Ed è proprio da queste considerazioni ed in questa direzione che l'Autorità intende muovere per affrontare la sfida offerta dal sempre più diffuso impiego di applicazioni per *smartphone*, adoperandosi concretamente - se del caso, anche mediante mirate campagne informative - per diffondere tra gli utenti una nuova cultura che tenga conto, oltre che delle affascinanti ed innovative possibilità rese accessibili dalle nuove tecnologie, anche di alcuni punti di particolare rilievo e delicatezza. Tra questi:

- il rischio cagionato dalla carenza di consapevolezza dell'utente in ordine a profili di assoluta rilevanza che lo riguardano in maniera diretta e possiedono potenziali attitudini lesive dei suoi diritti in materia di protezione dei dati personali;
- le specificità legate all'utilizzo di applicazioni, specie quelle ad opera di sviluppatori terzi, che raccolgono dati sulla vita privata (dai contatti alla posizione geografica, sino alle abitudini di consumi e comportamenti, a dati relativi alla salute ed alla vita di relazione);
- la possibilità che i soggetti che trattano le informazioni personali degli utenti, anche eventualmente di carattere sensibile, possano renderle "pubbliche" ovvero comunicarle ad altri soggetti determinati, sia per finalità commerciali che di altro genere, non specificamente correlate alla raccolta e, più in generale, non conformi ai desideri dell'utente medesimo, innanzitutto per l'indubbia attitudine dei dati a favorire attività di profilazione dell'utente;
- la possibilità che, in assenza di regole specifiche, i dati così raccolti possano essere archiviati sui sistemi del fornitore del servizio applicativo per periodi di tempo ultronei rispetto alla fornitura del servizio stesso, potenzialmente indeterminati; che, addirittura, possano continuare a costituire oggetto di trattamento perfino successivamente al momento in cui l'utente ha cessato di far ricorso ad una determinata applicazione ovvero di utilizzare uno specifico dispositivo.

Il duplice obiettivo di implementare sia la trasparenza nelle modalità di funzionamento delle applicazioni, con specifico riguardo al trattamento delle informazioni personali degli utenti, sia il controllo esercitabile, nonchè la dimensione

sovrana nazionale dei produttori e, in termini ancor più generali, il respiro globale del mercato delle *mobile apps*, suggeriscono di pensare alla possibile trasposizione degli interventi in un contesto più ampio di quello nazionale. Si potrebbe, cioè, ipotizzare un'azione sinergica con interlocutori, anche istituzionali, che operino in ambito comunitario.

Una prospettiva, questa, concretamente realizzabile, specie se si valuta lo specifico ruolo di mediazione assunto dai citati produttori di sistemi operativi che, essendo anche i gestori dei *market* ovvero dei cataloghi di applicazioni, hanno tra l'altro una capacità di interdizione nei confronti degli sviluppatori eventualmente inadempienti alle prescrizioni previste dalle disposizioni contrattuali (*Terms of Service*).

In tale quadro, più pregnanti garanzie per l'utente potranno essere ottenute attraverso una combinazione di accorgimenti tecnici - sufficientemente generali da non modificare le strategie di mercato ma comunque ragionevolmente efficaci - e di norme contrattualistiche da inserire negli accordi proposti dai gestori dei *market* e rivolti sia agli sviluppatori delle applicazioni che agli utenti finali.

Il futuro, insomma, è già incominciato.



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Cloud computing

Cloud computing: indicazioni per l'utilizzo consapevole dei servizi

Schede di documentazione



www.garanteprivacy.it



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Francesco Pizzetti, *Presidente*
Giuseppe Chiaravalloti, *Vice Presidente*
Mauro Paissan, *Componente*
Giuseppe Fortunato, *Componente*

Daniele De Paoli, *Segretario generale*

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 696773785
www.garanteprivacy.it

Cloud computing:
indicazioni per
l'utilizzo consapevole
dei servizi

PAGINA BIANCA

INDICE

- 1. Premessa*
- 2. Che cosa è il cloud computing?*
- 3. Esternalizzare i dati nelle cloud pubbliche*
- 4. I diversi modelli di servizio*
- 5. Innovare, governando i rischi*
- 6. Indicazioni per l'utilizzo consapevole dei servizi cloud*

PAGINA BIANCA

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 enunciate 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 importante 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 trattamento. 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;