Iusletter
informazione e aggiornamento giuridico

LaScala
STUDIO LEGALE

Focus on

IL DIRITTO NELLA SFIDA DELL'INNOVAZIONE TECNOLOGICA:

IL CLOUD COMPUTING

Febbraio 2017

www.lascalaw.com

www.iusletter.com

Milano | Roma | Torino | Bologna | Firenze | Ancona | Vicenza | Padova

redazione@iusletter.com

Scopo del presente contributo è quello di riflettere su alcuni importanti aspetti giuridici relativi al *cloud computing*, uno dei settori in cui è maggiormente possibile riscontrare il carattere evolutivo del diritto. La rapidissima crescita dell'utilizzo del *cloud* e l'analisi dei relativi rischi e problematicità suggeriscono agli utenti (privati, imprese o professionisti) di ottenere un'adeguata informazione riguardo ai servizi utilizzati ed evidenziano l'urgenza di un intervento legislativo a livello nazionale e internazionale volto a tutelare i diritti dei singoli.

1. Cenni introduttivi e definizione del fenomeno

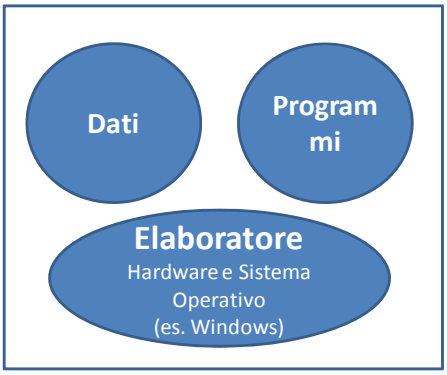
L'evoluzione delle tecnologie informatiche è in continuo sviluppo e ogni giorno vengono messi a disposizione degli utenti nuovi strumenti e soluzioni sempre più sofisticati che consentono di soddisfare le crescenti esigenze di informatizzazione e di comunicazione. In tale quadro il *cloud computing* è un insieme di servizi che più di altri si sta diffondendo con grande rapidità tra privati, imprese, pubbliche amministrazioni e professionisti.
Il termine *cloud computing* o *cloud* si riferisce a un insieme di tecnologie e di servizi che consentono il trasferimento della localizzazione dei *database*, dei processi di elaborazione e dei servizi di manutenzione dei dati in sistemi informatici gestiti da un soggetto terzo (il *cloud provider*), in modo da consentire la sincronizzazione dei file tra dispositivi diversi (pc, tablet, smartwatch, laptop, ecc.) caricandoli in remoto (sulle "nuvole") attraverso la rete internet senza dover implementare una rete interna complessa e costosa.

Spesso si utilizzano tecnologie *cloud* senza nemmeno rendersene conto (come avviene ad esempio con *iCloud*). Alcuni dei più diffusi servizi di posta elettronica, di elaborazione di testi e molte funzioni e applicazioni offerte dagli *smartphone* (ad esempio quelle che sfruttano la geolocalizzazione consigliando i locali o gli esercizi commerciali più vicini, che consentono di ascoltare musica o di accedere a giochi *on line*) sono basati sul *cloud*.

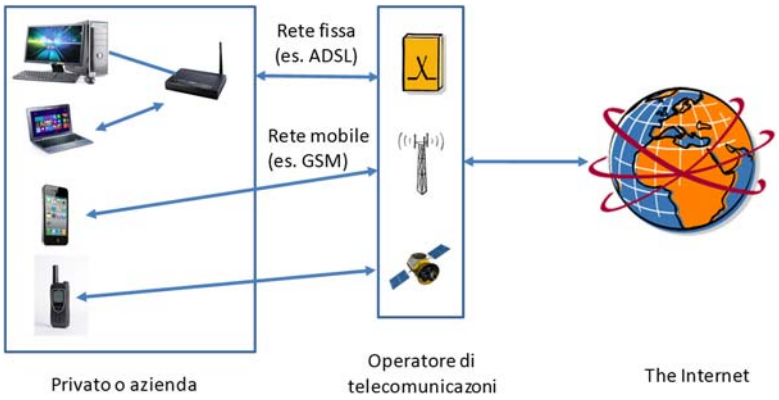
Il *cloud computing* ha costituito una radicale trasformazione rispetto all'utilizzo del singolo personal computer (si veda l'immagine (a)), con cui l'utente gestisce i propri dati isolatamente sul proprio apparecchio. Già con l'accesso alla rete Internet (b) – la quale, concepita in ambito

della Difesa degli Stati Uniti d'America con lo scopo di creare una rete di comunicazione fra i diversi terminali in modo che, qualora uno o più dei nodi della rete venisse distrutto, la rete si auto-riconfigurasse per garantire il regolare traffico fra i nodi sopravvissuti, consente di poter organizzare ed usufruire di svariati servizi in modo economico ed efficiente – il controllo della diffusione delle informazioni viene parzialmente perso e il controllo degli instradamenti del traffico non è più predeterminato ma si adatta dinamicamente in funzione del traffico e della configurazione della rete, anche se i nodi di elaborazione rimangono comunque localizzati e controllabili. Con il *cloud* (c) questo concetto di dinamicità del traffico viene esteso alla dinamicità di tutte le risorse della rete, siano esse capacità di elaborazione, memorizzazione o addirittura processi di elaborazione. La dislocazione fisica dei server presenti in una sottorete, peraltro, può essere sia internazionale che intercontinentale. Al di là delle diverse possibili classificazioni dei servizi *cloud*, tutti i servizi sono quindi accomunati dalla delocalizzazione dei dati che vengono immessi in uno spazio non immediatamente percepibile ed individuabile.

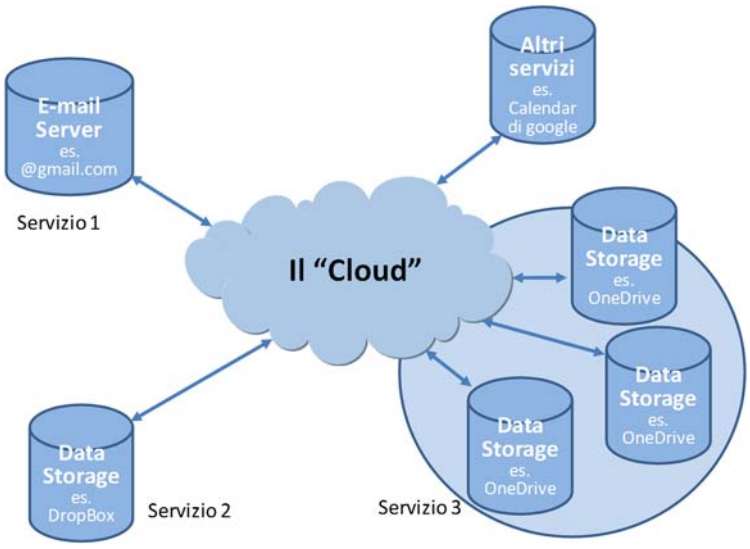
(a) Il Personal Computer



(b) L'accesso alla rete di telecomunicazioni e Internet



(c) Il *cloud*



Una principale classificazione del *cloud* attiene all'architettura della "nuvola" e alla gestione interna o esterna del trattamento dati e al modello di servizio offerto al cliente[1]:

1. Il ***private cloud*** è un'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. I *private cloud* possono essere paragonati ai tradizionali data center nei quali, però, vengono impiegati alcuni accorgimenti tecnologici che permettono di ottimizzare l'utilizzo delle risorse disponibili e di potenziarle agevolmente in caso di necessità;

2. il ***public cloud*** è un'infrastruttura 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 dei 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 adottata 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;

3. altre nuvole; esistono altri tipi di nuvole con caratteristiche miste, quali gli ***hybrid cloud***, caratterizzati da soluzioni che prevedono l'utilizzo di servizi erogati da infrastrutture private accanto a servizi acquisiti da *cloud* pubblici, e i ***community cloud***, in cui l'infrastruttura è condivisa da diverse organizzazioni a beneficio di una specifica comunità di utenti.

[1] Si vedano a riguardo: Garante per la protezione dei dati personali, *Cloud computing. Proteggere i dati per non cadere dalle nuvole* e *Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*.

A seconda, poi, delle esigenze dell'utente, sono disponibili varie soluzioni di *cloud* erogate secondo modalità che possono essere classificate in diverse categorie, dette "modelli di servizio"[2].

2. Vantaggi e problematicità

Il *cloud computing* favorisce e migliora le interazioni professionali e sociali e offre considerevoli vantaggi a livello economico, organizzativo e di sicurezza.

Quanto ai vantaggi economici, il *cloud* consente di usufruire di servizi complessi senza doversi necessariamente dotare di altri hardware avanzati: 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; è inoltre possibile configurare, espandere e accedere a risorse *on demand* con molta facilità. Quanto ai vantaggi organizzativi, il *cloud* consente di usufruire di tali servizi senza doversi dotare di personale in grado di programmare o gestire il sistema. Il *cloud computing* può anche offrire vantaggi in termini di sicurezza, in quanto i *cloud provider* sono in grado di offrire altissimi livelli di sicurezza (continuità del servizio e back-up periodico e geografico) ad un prezzo accessibile.

Tuttavia, l'utilizzo delle tecnologie *cloud* presenta al tempo stesso criticità e rischi, di cui è bene tenere conto.

Oltre ai rischi legati alla perdita di controllo sui propri dati, è ben possibile che si presentino problemi dovuti, ad esempio, al malfunzionamento o all'hackeraggio del servizio che potrebbero causare l'indisponibilità (anche solo temporanea) dei dati o addirittura la loro perdita. Inoltre, un eventuale malfunzionamento potrebbe colpire contemporaneamente un numero elevato di servizi condivisi. Il servizio virtuale potrebbe, poi, in assenza di adeguate garanzie in merito alla

[2] *Cloud Infrastructure as a Service* (IaaS – infrastruttura *cloud* resa disponibile come servizio); *Cloud Software as a Service* (SaaS – software erogato come servizio del *cloud*); *Cloud Platform as a Service* (Paas – piattaforme software fornite via Internet come servizio).

qualità della connettività di rete, risultare degradato in presenza di elevati picchi di traffico o addirittura indisponibile laddove si verifichino eventi anomali[3].

Appare pertanto opportuna una attenta ponderazione in ordine all'utilizzo dei servizi *cloud* per conoscerne le potenzialità ma anche le criticità, se si considera oltretutto che solitamente i contratti conclusi con i *cloud provider* costituiscono contratti per adesione, le cui condizioni sono stabilite a priori dal *provider* senza che avvenga una relativa negoziazione con l'utente.

A tal proposito, il 7 luglio 2012 il Working Party 29 (il gruppo di lavoro dei Garanti Privacy che si riunisce a Bruxelles) ha adottato un parere sul *cloud computing* in cui si afferma chiaramente che "*imprese e amministrazioni che intendono utilizzare servizi di* cloud computing *dovrebbero innanzitutto effettuare un'analisi del rischio completa e approfondita. Tutti i fornitori di servizi* cloud *nel SEE dovrebbero fornire al cliente tutte le informazioni necessarie per valutare correttamente i pro e i contro dell'adozione di un simile servizio. Sicurezza, trasparenza e certezza giuridica per i clienti dovrebbero essere i principi fondamentali alla base dell'offerta di servizi di* cloud computing"[4].

3. Il diritto nella sfida dell'innovazione tecnologica

Quello dell'informatica è uno degli ambiti in cui è maggiormente possibile riscontrare il carattere evolutivo del diritto. L'intenso dinamismo della tecnologia non consente alcuna cristallizzazione normativa, imponendo la necessità di un quadro di principi e di regole volto a segnare il raccordo tra il progresso tecnologico e la tutela dei diritti della persona, atteso che la scienza si pone al servizio dell'uomo e i diritti fondamentali degli individui non possono essere sacrificati in nome

[3] «*Google Drive non ha funzionato correttamente per alcune ore. A segnalarlo sono stati gli utenti del cloud di Big G che hanno chiesto spiegazioni all'azienda sul forum dei suoi prodotti. Chi utilizza la piattaforma non riusciva a modificare le proprie cartelle in Drive, cancellare i contenuti caricati o crearne di nuovi. Accedendo al proprio cloud si potevano caricare file solo nell'Home di Drive, al di fuori delle cartelle, anche se alcuni segnalavano la possibilità di caricare file all'interno delle cartelle trascinandoli direttamente dal proprio pc. Probabilmente si è trattato di un bug che ha colpito la piattaforma di archiviazione di Google*». www.repubblica.it, 4.04.2016. «*Google ha dichiarato che in uno dei suoi data center in Belgio i dati sono stati cancellati dai dischi dopo che un disco è stato colpito quattro volte da un fulmine. Alcune persone hanno conseguentemente perso l'accesso ai propri file in modo permanente*». www.bbc.com, 19.08.2015.

[4] Atti del Working Party 29.

del progresso scientifico[5]. Del resto, la tecnologia *cloud* procede molto più velocemente dell'attività del legislatore, non solo in Italia ma in tutto il mondo, e manca ancora un quadro normativo – nazionale e internazionale – che tenga conto di tutte le novità introdotte dal *cloud computing* e che sia in grado di offrire tutele adeguate rispetto alle fattispecie giuridiche connesse all'adozione di servizi di elaborazione e di conservazione dei dati[6]. Come muoversi in questo ambiente complesso ed instabile?

Si procede ora con l'analisi di due distinte tematiche giuridiche: la tutela dei dati personali e la tutela della proprietà intellettuale delle opere immesse in *cloud*.

3.1 La *privacy* nel *cloud computing*

Considerando che la nascita delle nuove tecnologie *cloud* favorisce lo sviluppo di una mole impressionante di dati di vario genere accessibili nelle varie nuvole e i rispettivi gestori saranno i soggetti depositari di una quantità sterminata di informazioni, che cosa ne sarà delle *privacy* dei vari utenti che sceglieranno e stanno già scegliendo di ricorrere al *cloud*?[7]

I rischi per i soggetti che decidono di affidarsi al *cloud* sono molteplici e la cautela e un'informazione adeguata rispetto ai servizi si rende doverosa sotto diversi aspetti. Si pensi ad esempio alle gravi conseguenze per un'impresa in caso di fallimento del *provider*: quale sarebbe la sorte dei dati aziendali? Quanto invece all'ambito legale, gli avvocati che ricorrono al *cloud* dovrebbero fornire apposita informativa ai propri clienti rendendoli edotti del fatto che i relativi dati vengono caricati sulle nuvole.

---

[5] "*È necessario che si crei un equilibrio virtuoso tra l'espansione economica e le garanzie per i soggetti destinatari degli impulsi che spingono le innovazioni*". G. Santaniello, *Tipologia delle innovazioni tecnologiche e protezione dei dati personali*, intervento al Convegno *Innovazioni tecnologiche e privacy*, Roma 2004 presso il Garante per la protezione dei dati personali.

[6] Il trattamento dei dati al di fuori dei confini nazionali e, dunque, al di là dei poteri delle Autorità nazionali di controllo introduce, peraltro, la problematica della legge applicabile. "*Per anni [...] sembrava [...] che il cloud fosse una sorta di terra di nessuno. [...] Gli esperti di diritto per anni hanno posto domande, organizzato convegni, cercato di approfondire il tema soprattutto dal punto di vista tecnico, ma la risposta classica era che il significato di cloud, non solo letterale, era proprio nuvola e quindi luogo-non-luogo in cui non si poteva nemmeno immaginare di poter applicare delle leggi*" B. Del Genio, *La Protezione dei dati personali nel cloud*.

[7] R. Razzante, *Manuale di diritto dell'informazione e della comunicazione*, Cedam, Padova 2013, 483.

Il rischio maggiore per la *privacy* deriva dalla delocalizzazione dei dati, che possono essere esportati da un sistema *cloud* ad un altro. La maggior parte dei *cloud provider* ha sede all'estero, e così i loro server, e non sono facilmente individuabili. La possibilità di conservare i dati in luoghi geografici differenti, pone problemi attinenti sia alla normativa applicabile in caso di contenzioso fra utente e fornitore, sia in relazione alle disposizioni nazionali che disciplinano il trattamento, l'archiviazione e la sicurezza dei dati, che potrebbero non offrire garanzie di sicurezza adeguate e che dovrebbero, in ogni caso, coordinarsi con la normativa europea, ove applicabile.

La maggioranza dei rischi del *cloud computing* per la protezione dei dati personali rientra, quindi, in due ampie categorie, e precisamente la mancanza di controllo sui dati e la carenza di informazioni concernenti il trattamento stesso (assenza di trasparenza). Quanto al primo rischio, affidando dati personali a sistemi gestiti da un fornitore di servizi *cloud*, gli utenti rischiano di perdere il controllo esclusivo dei dati e di non poter prendere le misure tecniche e organizzative necessarie per garantire la disponibilità, l'integrità, la riservatezza, l'isolamento, la portabilità dei dati e la possibilità di intervento sugli stessi. Quanto, poi, alla trasparenza, la disponibilità di informazioni insufficienti sulle operazioni di trattamento nei servizi *cloud* rappresenta un rischio per i responsabili del trattamento e per gli interessati, che potrebbero non essere consapevoli di potenziali rischi e minacce, non potendo pertanto prendere misure appropriate.

Risulta quindi necessario individuare chi rivesta i ruoli di "Titolare" e di "Responsabile del trattamento" dei dati, poiché tale individuazione comporta precise conseguenze in termini di individuazione delle responsabilità in capo a ciascun soggetto.

In Italia, il Garante della Privacy ha fornito indicazioni e prescrizioni relativamente agli aspetti del trattamento dei dati personali nel *cloud computing*, determinando le principali caratteristiche grazie alle quali è possibile identificare il Titolare ed il Responsabile del trattamento. Ai sensi dell'art. 28 del Codice della Privacy, il Titolare del trattamento è colui che "*esercita un potere decisionale del tutto autonomo sulle finalità e modalità del trattamento, ivi compreso il profilo della sicurezza*". Tuttavia la norma citata deve essere letta in combinato disposto con gli articoli

11 e 29 dello stesso Codice, dove si rinvengono alcune linee guida circa le modalità del trattamento dei dati personali che consentono di identificare nel titolare colui che determina le finalità del trattamento, determina le modalità essenziali del trattamento, ha poteri di verifiche periodiche sul Responsabile del trattamento e può fornire informazioni scritte al Responsabile del Trattamento. Questi compiti sembrano incompatibili con il ruolo del semplice utilizzatore e fanno propendere per la soluzione della contitolarità del trattamento dell'utilizzatore e del *cloud provider*. Una recente dottrina sottolinea che il *cloud provider* può certamente avere un proprio ruolo autonomo rispetto all'utente relativamente ai profili di gestione della sicurezza dei dati[8], assumendo, quindi, la responsabilità verso l'interessato di preservare la riservatezza, l'integrità e la disponibilità dei dati, obblighi peraltro commisurati al tipo di servizio offerto ed al regime contrattuale adottato. Il Codice Privacy individua alcune misure minime la cui adozione è obbligatoria e presidiata da apposite sanzioni, disponendo, all'art. 31, l'obbligo di adeguamento del trattamento in base all'evoluzione tecnologica[9].

Il ruolo del *cloud provider* è stato oggetto di interesse da parte dei Garanti Privacy a livello nazionale ed internazionale. In particolare, il Garante italiano, tra gli aspetti critici legati alla sicurezza dei dati personali, ha individuato quelli che necessitano di specifica attenzione[10]. L'utente, infatti, affida i propri dati ai sistemi di un fornitore remoto, perdendone il controllo diretto ed esclusivo, affidando la riservatezza e la disponibilità delle informazioni allocate sulla nuvola ai meccanismi di sicurezza adottati dal *service provider*. I dati personali potrebbero,

---

[8] P.Balboni, L.Bolognini, D.Fulco, E.Pelino, *Cloud computing e tutela dei dati personali in Italia. Una sfida d'esempio per l'Europa*, in Diritto, Economia e Tecnologie della Privacy, 2011.

[9] "*I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*". Art. 31 D.Lgs. 196/2003.

[10] "*I trattamenti di dati personali richiedono, infatti, una ponderazione dei rischi legati alla sicurezza ed alla fruibilità delle informazioni. 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 nei casi di 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*". Garante per la Protezione dei Dati Personali, 23.06.11, scheda di documentazione "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*", doc. web n. 1819933.

inoltre, passare per una catena di trasformazione dei servizi acquisiti presso altri *service provider*, diversi dal fornitore con cui l'utente ha stipulato il contratto, col rischio di non sapere quale dei gestori intermedi possa accedere ai dati. 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 subfornitori dei quali il *cloud provider* potrebbe avvalersi, oltre che sul luogo di conservazione dei dati.

La normativa nazionale deve venire necessariamente coordinata con la normativa internazionale. A ragione si è sottolineato che "*l'evoluzione normativa della materia non può affidarsi a una fonte legislativa monocentrica, bensì a un policentrismo di fonti collocate in una coordinata sequenza a vari livelli (una cornice legislativa concertata tra tutti i Paesi interessati alla soluzione del problema e, in aderenza a essa, la specificazione di regole mediante leggi nazionali, a seconda delle varie aree geografiche, e inoltre l'adozione di codici-modello di formazione autodisciplinare). Si realizza in tal modo quel moderno processo regolatore, frutto della convergenza di molteplici fonti normative*"[11].

In tal senso si auspica un rapido intervento legislativo che adegui la normativa vigente all'evoluzione tecnologica e che sia volto, nel contempo, a tutelare la *privacy* degli utenti dei servizi.

3.2 Cloud computing e tutela della proprietà intellettuale

La tutela dei frutti dell'attività creativa e inventiva di privati, imprese e professionisti assume un rilievo decisivo nel contesto dell'innovazione tecnologica, e in particolare, nel caso di immissione dei dati nel *cloud*.

Si pensi ad un'impresa che salvi in *cloud* la documentazione relativa alle proprie invenzioni industriali, ad un avvocato che salvi in *cloud* un proprio lavoro o ancora ad un dottorando che

[11] G. Santaniello, *Tipologia delle innovazioni tecnologiche e protezione dei dati personali*, 26, in "Innovazioni tecnologiche e privacy" a cura di G. Rasi.

salvi in *cloud* la propria tesi non ancora discussa e pubblicata. Tutti questi soggetti hanno un grande interesse a che tali opere dell'ingegno vengano tutelate.

Occorre, pertanto, verificare le forme di tutela previste dai *cloud provider* relativamente alla proprietà intellettuale degli utenti del servizio, attraverso l'analisi delle relative previsioni contrattuali[12].

I termini di servizio di Google Drive[13], ad esempio, recano l'articolo rubricato "*I contenuti dell'utente nei nostri Servizi*", che prevede che a fronte dell'utilizzo di alcuni servizi, tra i quali il *cloud*, l'utente "*mantiene gli eventuali diritti di proprietà intellettuale detenuti sui propri contenuti*". Viene così chiarito che i diritti di privativa restano in capo all'utente, il quale non attua alcuna cessione in favore del fornitore, configurandosi una mera licenza ovvero un'autorizzazione al godimento dei contenuti caricati, limitata nel tempo, nel territorio, negli usi, limitatamente allo scopo esclusivo di "*utilizzare, promuovere e migliorare*" i servizi e di "*sviluppare*" nuovi servizi. Ciò potrebbe comportare l'utilizzo da parte di Google dei contenuti caricati dall'utente a scopo pubblicitario (se, per esempio, dall'esame dei file caricati in Google Drive emerge un particolare interesse per una specifica tipologia di abbigliamento, l'utente potrebbe ricevere pubblicità mirata a questo scopo). Inoltre la licenza prosegue altresì nel caso in cui "*l'utente smette di utilizzare*" il servizio *cloud*, sebbene sia previsto che "*In caso di interruzione della fornitura di un Servizio, ove ragionevolmente possibile, offriremo all'utente un ragionevole preavviso e la possibilità di rimuovere le informazioni da tale Servizio*". Occorre tuttavia considerare che i servizi *cloud* dispongono di una funzione che consente loro di poter risalire a versioni precedenti dei file quanto caricato, anche se successivamente rimossi dall'utente ed utilizzare così i dati per lo sfruttamento pattuito in licenza. Analogamente avviene con il contratto del servizio Dropbox[14], secondo il quale, peraltro, la licenza è concessa anche a

---

[12] Vedasi anche: A. Michinelli, *Cloud computing e condizioni contrattuali: un regalo ai giganti del web?* in Altalex, 27.07.2016; A. Stazi, D. Mula, *Titolarità e contitolarità dei diritti IP nei sistemi di "crowdsourcing, open source e cloud computing"*. Relazione al Convegno "Le innovazioni del nuovo web", Parma, 31.10.2014, in Il Diritto industriale, 2015, fasc. 2, 149-154; G. Colangelo, *L'"enforcement" del diritto d'autore nei servizi "cloud"*. Relazione al Convegno "L'enforcement del diritto d'autore nei Servizi Cloud", Associazione Letteraria e Artistica Internazionale, Milano, 20.06.2012, in Il Diritto d'autore, 2012, fasc. 2, 174-205.

[13] Vedasi: https://www.google.com/policies/terms. Trattasi, invero, di contratto generale multiservizi nel quale si rinvengono alcune clausole applicabili al servizio Drive.

[14] Vedasi: https://www.dropbox.com/terms2014.

terzi "*collaboratori*" del *provider*, senza che ne venga precisata l'identità, e secondo cui in caso di mancato accesso al servizio per un periodo di almeno dodici mesi consecutivi, l'utente rischia di perdere definitivamente i propri contenuti.

Nel complesso, dunque, mentre da un lato viene garantita la titolarità dei contenuti in capo all'utente, dall'altro lato la possibilità dei *provider* di utilizzare e cancellare i dati comporta di fatto uno svuotamento di contenuto dei diritti dell'utente. Anche su tale aspetto, quindi, si impone un intervento attento del legislatore, atto a prevedere una tutela effettiva e completa dei diritti degli utenti.

4. Considerazioni finali

L'emergenza del fenomeno del *cloud computing* sta avendo un impatto sociale ed economico talmente rilevante da rendere necessario e non ulteriormente differibile un intervento legislativo che, a livello nazionale ed internazionale, consenta di adeguare le regole e le categorie giuridiche esistenti all'evoluzione tecnologica, nel bilanciamento degli interessi dei singoli. Nell'attesa di un intervento legislativo attento, un'adeguata informazione in ordine ai servizi utilizzati potrà scongiurare l'insorgere di rischi gravosi a carico degli utenti.

Orsolina Fortini – o.fortini@lascalaw.com