GIUSTIZIA CIVILE.com

Cloud computing e protezione dei dati nel web 3.0

di **Guido Noto La Diega**

Approfondimento del 05 aprile 2014

ISSN: 2284-3760

Il *cloud computing* è un ritrovato deputato all'archiviazione, elaborazione e uso di dati su computer remoti, grazie al quale gli utenti hanno a disposizione una potenza di elaborazione quasi illimitata, non sono tenuti ad investire grandi capitali per soddisfare le proprie esigenze e possono accedere ai loro dati ovunque sia disponibile una connessione Internet. Il presente scritto si propone di contribuire ad una migliore comprensione della nuova tecnologia e alla ricostruzione dell'attuale (invero scarno) quadro giuridico, ciò che può aiutare a superare i principali problemi posti dalla nuvola al diritto dei privati e riconducibili, primariamente, alla protezione dei dati, al diritto dei contratti e agli IPRs. Dando conto dei principali atti normativi italiani ed europei in materia, ci si concentrerà soprattutto sul primo profilo per almeno due ordini di ragioni, variamente interrelate. Da una parte, perché, pur mancando una disciplina organica che risolva tutte le questioni giuridiche connesse al *cloud*, uno studio complessivo dei frammenti normativi rivela che il campo della protezione dei dati è quello in cui la produzione normativa è più cospicua. Dall'altra parte, perché le paure circa la sicurezza dei dati archiviati nella nuvola costituiscono il principale freno alla diffusione della tecnologia in esame. Nonostante la dimostrata rilevanza del *cloud*, è stato notato che i legislatori e le istituzioni sono ancora confusi su ciò che la nuvola informatica realmente può significare per la società dell'informazione: i giuristi sono quindi chiamati al compito improcrastinabile di (ri)costruire un *framework* normativo adeguato alle nuove sfide, tale da resistere al «*digital tsunami*», non rinunciando a preservare la coerenza del sistema.

SOMMARIO: 1. Cenni introduttivi. - 2. Il cloud computing e la protezione dei dati nel diritto italiano. - 3. Il diritto privato europeo fra le nuvole - 4. Osservazioni conclusive.

1. Cenni introduttivi.

Il *cloud computing* è un ritrovato deputato alla «*archiviazione, l'elaborazione e l'uso di dati su computer remoti* [grazie al quale] gli utenti hanno a disposizione una potenza di elaborazione quasi illimitata, non sono tenuti ad investire grandi capitali per soddisfare le proprie esigenze e possono accedere ai loro dati ovunque sia disponibile una connessione Internet» [1]. Il presente scritto si propone di contribuire ad una migliore comprensione della nuova tecnologia e alla ricostruzione dell'attuale (invero scarno) quadro giuridico, ciò che può aiutare a superare i principali problemi posti dalla nuvola al diritto dei privati e riconducibili, primariamente, alla protezione dei dati, al diritto dei contratti e agli IPRs.

Ci si concentrerà soprattutto sul primo profilo – la riservatezza – per almeno due ordini di ragioni, variamente interrelate. Da una parte, perché, pur mancando una disciplina organica che risolva tutte le questioni giuridiche connesse al *cloud*, uno studio complessivo dei frammenti normativi rivela che il campo della protezione dei dati è quello in cui la produzione normativa è più cospicua. Dall'altra parte, perché le paure circa la sicurezza dei dati archiviati nella nuvola costituiscono il principale freno alla diffusione della tecnologia in esame [2]. Si sente sovente dire che nell'attuale fase dell'era digitale la riservatezza è un diritto costantemente minacciato e che, come è stato autorevolmente scritto, va reinventato «nell'età nuova del Web, della continua e massiccia produzione di profili, del *cloud computing,* dell'intelligenza artificiale, di sviluppi come quelli indicati dall'*automatic computing*» [3]. Una reinvenzione del concetto di protezione dei dati personali si impone «non solo perché viene esplicitamente considerato come un autonomo diritto fondamentale, ma perché si presenta come strumento indispensabile per il libero sviluppo della personalità e per definire l'insieme delle relazioni sociali» [4], rafforzando così la costituzionalizzazione della persona.

Il *cloud computing* è in costante crescita, come dimostra, fra l'altro, il proliferare di programmi come Dropbox, Google Drive, iCloud e SkyDrive (da febbraio 2014 OneDrive) e nuovi *cloud providers* «*popping up everywhere*» [5]. Esso, peraltro, è tanto rilevante da segnare, come meglio si vedrà, l'ingresso nel *web* 3.0, la terza fase di Internet [6] e alimentare un mercato da seimiladuecento miliardi di euro [7]; ma sinora non ha suscitato, di là dallo steccato di ingegneri e informatici [8], l'attenzione che, invece, merita, come posto in luce recentemente anche da uno studio voluto dalla Commissione europea [9] e da parte della dottrina [10].

Se sviluppi quali il *peer-to-peer*, lo *streaming*, i *social networks* e il *free and open source software* (FOSS) rappresentano senz'altro importanti novità del nostro tempo, si può dire che il *cloud computing* segni l'ingresso nella terza fase di Internet, costituendo un'invenzione tanto rivoluzionaria quanto il *World Wide Web.* Nella prima fase, programmi per elaboratore e sistemi operativi erano combinati per creare un semplice flusso di comunicazioni (ad es., per inviare email); la seconda fase è dominata dalla menzionata invenzione di Tim Berners-Lee, che rese possibile l'accesso a milioni di siti; la terza è, appunto, quello per cui dati, opere e programmi sono creati, conservati e gestiti nella nuvola informatica. Ferma l'importanza del *cloud*, forse è eccessivo l'accostamento alla raffigurazione data da Averroè all'immortalità, «intelletto comune superindividuale, separato dalle anime individuali che in esso si immergono e da esso attingono» [11].

La tenzone fra tecnologia e diritto oggi si fa singolare. A mo' d'esempio, si pensi che la possibilità di acquistare programmi per elaboratore per via di *download* aveva già prodotto l'evaporazione del *corpus mechanicum*: allora, però, bisognava pur sempre passare da un computer, ora ci si sta emancipando anche dall'*hardware*.

Il suo sviluppo, a parere di chi scrive [12], è da ricollegare essenzialmente a quattro fattori: a. la proliferazione di dispositivi portatili con accesso a Internet, che consentono di lavorare allo stesso *file* da diverse postazioni; b. la diminuzione della memoria interna dei dispositivi, a fronte del crescente bisogno di spazio di immagazzinamento; c. la diffusione della banda larga e consimili connessioni veloci, senza la quale servizi come il *cloud computing* non potrebbero neanche essere concepiti; d. la possibilità, specialmente per le aziende, di ottenere risparmi di costi grazie alle economie di scala connesse all'esternalizzazione e centralizzazione dell'archiviazione e lavorazione dei dati, con grandi vantaggi in termini di competitività [13].

Grazie ai nuovi paradigmi introdotti dal *cloud computing*, Internet diviene una piattaforma non più deputata esclusivamente alle comunicazioni, ma anche alla creazione, lavorazione e archiviazione di dati della più varia natura. Si tratta di un «*many-to-many medium that can link millions of users to thousands of computers simultaneously [and] represents a fundamental shift in how computing is done*» [14]. In altri termini, per dirla col CEO

di Google, «*we're moving into the era of 'cloud' computing, with information and applications hosted in the diffuse atmosphere of cyberspace rather than on specific processors and silicon racks. The network will truly be the computer*» [15]. Non è un caso che anche gli studiosi degli IPRs più attenti rilevino come il «*cloud computing* sembr[i] destinato a sconvolgere l'orizzonte di riferimento più di quanto abbiano fatto i noti casi *Napster* e *Grokster*» [16].
Ora,le caratteristiche principali del ritrovato tecnologico in esame sono, essenzialmente, cinque: l'*on-demand self-service*, il *broad network access*, il *resource pooling*, la *rapid elasticity* e il *measured service*. Quindi, l'utente ha la possibilità di procurarsi autonomamente (l'*on-demand self-service*) capacità di computazione senza richiedere interazione umana con ogni *service provider*; le funzionalità sono disponibili nella rete e accessibili mediante meccanismi standard (*broad network access*) che promuovono un uso da parte di piattaforme eterogenee; le risorse di computazione del *provider* sono raggruppate (*resource pooling*) per servire molteplici utenti, usando un modello *multi-tenant*, con differenti risorse fisiche e virtuali assegnate dinamicamente a seconda della richiesta dell'utente; e, quanto alla quarta caratteristica (*rapid elasticità*), le funzionalità possono essere fornite elasticamente, in alcuni casi automaticamente, per rispondere rapidamente in modo scalare proporzionalmente alla richiesta. Circa l'ultimo profilo (*measured service*), infine, è da dire che i sistemi *cloud* controllano automaticamente e ottimizzano l'uso delle risorse facendo leva su capacità di misurazione al livello di astrazione appropriato al tipo di servizio: l'uso delle risorse può essere, così, monitorato contribuendo alla trasparenza, tanto per il *provider* quanto per l'utente.
I servizi *cloud*, poi, seguono tre modelli fondamentali: *Software as a Service* (SaaS), *Platform as a Service* (PaaS) e *Infrastructure as a Service* (IaaS). Nel SaaS, il *provider* mette a disposizione degli utenti, dietro corrispettivo, applicazioni fruibili direttamente in linea, senza necessità di ottenere una licenza di *software* o comunque di istallare lo stesso sul proprio dispositivo [17]. Quando si tratta, invece, di PaaS il *provider* mette a disposizione l'*hardware* e una piattaforma inclusiva di OS, *middleware* e ambiente *runtime* [18]. Infine, il *provider*, nel caso si opti per l'Iaas, fornisce *server*, *router*, spazio di archiviazione, *hardware* e *software*, che l'utente può implementare includendo sistemi operativi ed applicazioni [19].
La distinzione più diffusa è quella fra *private cloud*, *community cloud*, *public cloud* e *hybrid cloud* [20]. Il primo *deployment model* è il preferito dalle imprese per la maggiori garanzie di protezione dei dati [21]ed è caratterizzato dall'uso esclusivo da parte di una singola organizzazione comprendente molteplici consumatori. Nel *community cloud*,invece,l'infrastruttura è fornita per l'uso esclusivo da una specifica comunità di consumatori appartenenti ad organizzazioni aventi interessi comuni(ad es., *mission* e *policy*). In entrambi i casi, l'infrastruttura può essere posseduta e gestita dall'organizzazione (ad una o più se è una nuvola comunitaria), da terzi o da combinazioni fra questi. Quanto, poi al *public cloud*, essoè caratterizzato da un'infrastruttura fornita per uso aperto al pubblico, che può essere posseduta e gestita da organizzazioni finanziarie, accademiche o istituzionali, o da combinazioni di queste. L'Agenzia per l'Italia digitale, nell'aggiornamento 2013 alle *Linee guida per il* disaster recovery *nelle pubbliche amministrazioni*, ha sottolineato che un aspetto cui bisogna prestare particolare attenzione, in quanto connesso alle peculiarità dei servizi *cloud*, è la «natura intrinsecamente multi utente dei servizi *public cloud*» (§ 4.3.2.2). La nuvola ibrida, invece, risulta dall'unione di due o più distinte infrastrutture *cloud* (*private*, *community* o *public*) che rimangono entità distinte, ma sono legate da tecnologie che rendono possibile la portabilità di dati e applicazioni.
Un'altra possibile classificazione, particolarmente rilevante visto il *focus* qui scelto, è quella incentrata sul livello di sicurezza dei dati nella nuvola. Da questo punto di vista, proposto nelle citate *Linee guida per il* disaster recovery, si individuano tre tipi di *cloud sites*: caldo, tiepido e freddo. Nel *hot cloud site*, le macchine virtuali sono sempre attive nella nuvola con replica in tempo reale delle macchine medesime tra sito di produzione e infrastruttura *cloud*. Nel sito tiepido, invece, sono presenti copie non in linea delle macchine virtuali attivabili in caso di disastro o per attività di test con tempi di ripristino di poche ore. Quanto, infine, al *cold cloud site*, nella nuvola sono conservati i *backup* dei sistemi di produzione che possono essere convertiti in macchine virtuali prima del ripristino al momento del disastro (v'è altresì la possibilità che l'utente trasferisca nella infrastruttura *cloud* al momento del disastro e del ripristino le immagini e i dati conservati su nastro o disco in altri siti).
Traendo le somme, si sta passando progressivamente dal classico metodo di salvataggio dei dati e gestione degli stessi sul *desktop – rectius*, nella memoria del computer – allo *storage* ed *editing* direttamente sul *cloud top* [22],

che consente di accedere ai propri archivi tramite qualsiasi dispositivo dotato di accesso Internet – dagli *smartphone* ai *tablet* – e favorendo i lavori di squadra, grazie all'uso di cartelle condivise, in un'ottica di *openness* per cui ognuno lavora sulla versione modificata dall'altro. Il nesso fra sistemi aperti e nuvola è alla base, fra l'altro, della recente decisione di Google di non citare più in giudizio i titolari di prodotti *open source* per rivendicare brevetti specifici, riservandosi solo, ovviamente, il diritto di difesa qualora fosse da questi convenuta. La scelta è stata motivata con la convinzione che i *free/open source softwares* (FOSS) siano vincenti, dato dimostrato dalla circostanza che «il *software open-source* è stato alla base di molte innovazioni nel *cloud computing*, nel *web* mobile, e in Internet in generale» [23].
Arrestandoci qui per ragioni di sintesi, si procederà a ricostruire il quadro giuridico vigente in materia di *cloud*, evidenziando i profili d'interesse per la protezione dei dati. Si intende dar conto del diritto interno (centrale e regionale) ed europeo, non trascurando il *soft law*, nel senso di atti, come le determinazioni delle autorità amministrative dipendenti o le comunicazioni della Commissione, che pur non avendo i crismi della legge (almeno in una concezione epistemologica di stretta osservanza giuspositivistica), influiscono profondamente nella vita dei consociati.

2. Il cloud computing e la protezione dei dati nel diritto italiano.
Mentre la giurisprudenza italiana non si è ancora confrontata col tema, di esso si registrano le prime tracce di diritto positivo già nel 2012. In ordine di tempo, l'ultimo intervento rilevante in materia di *cloud computing* era stato introdotto col d.l. 69 del 2013 (c.d. decreto del fare) e contemplava l'uso della nuvolaper l'*e-Health* sotto forma di fascicolo sanitario elettronico. L'imperfetto è d'obbligo, considerato che la l. n. 98 del 2013 di conversione del citato decreto non reca più traccia alcuna del riferimento alla nuova tecnologia. Un'occasione mancata.
Ciò posto, può stupire che gli strumenti legislativi tradizionali abbiano trascurato l'aspetto della protezione dei dati, che, come visto, è al centro delle preoccupazioni di imprese e consumatori. Le normative (*rectius*,i frammenti normativi) vigenti, sono, infatti fondamentalmente riconducibili agli obiettivi di aumentare l'efficienza della P.A (d.l. n. 179 del 2012, conv. in l. n. 221 del 2012, c.d. decreto crescita 2.0, che ha modificato d.lgs. n. 82 del 2005, codice dell'amministrazione digitale; l.r. Puglia n. 20 del 2012; del.g.reg. Toscana n. 40 del 2013; del.g.reg. Campania n. 501 del 2013), innovare l'istruzione (acc. n. 118/CSR del 2012; d. interm. 28 marzo 2012; d.l. n. 5 del 2012 conv. in l. n. 35 del 2012; del.g.reg. Marche n. 1259/2012), investire nel settore ricerca e sviluppo (R&S) (d. dir. 30 maggio 2012 e d. dir. 2 marzo 2012), promuovere gli attori deboli del mercato (in Friuli-Venezia Giulia la l.r. n. 27 del 2012 e i d.P.Reg. n. 27 del 2013 e n. 150 del 2013, in Veneto il d.dir. 2 maggio 2011, n. 9) e rendere effettivo il diritto fondamentale all'accesso ad Internet (l.r. Umbria n. 31 del 2013, sulla scorta del reg. 1316 del 2013).
E, allora, l'attenzione per le determinazioni di autorità amministrative indipendenti e agenzie non si impone solo in considerazione del rilevante fenomeno della c.d. «amministrativizzazione del diritto» [24], ma anche perché è in quegli strumenti, trascurati dalle impostazioni dottrinali più tradizionaliste, che si rinvengono gli approfondimenti maggiori del fenomeno *cloud*. In essi la questione della protezione dei dati emerge come nodale.
È con la com. 24 luglio 2013 che la Banca d'Italia affronta per la prima volta le questioni connesse alla nuvola. In particolare, si è provveduto a inserire nel titolo V della circ. n. 263 del 2006, recante «Nuove disposizioni di vigilanza prudenziale per le banche», i capitoli da 7 a 9, concernenti il sistema dei controlli interni, il sistema informativo e la continuità operativa. L'aggiornamento qui interessa, soprattutto, per l'ottavo capitolo, che innova radicalmente in materia di *governance* e organizzazione del sistema informativo, gestione del rischio informatico e requisiti per assicurare la sicurezza informatica e il sistema di gestione dei dati. Si prevede, fra l'altro, che nella definizione dei presidi di sicurezza per l'accesso a sistemi e servizi critici tramite Internet trovino applicazione le Raccomandazioni della BCE in materia di sicurezza dei pagamenti in internet. È, però, alla sez. VI sull'esternalizzazione del sistema informativo – le cui norme si applicano ai casi di *full outsourcing* o di esternalizzazione di componenti critiche del sistema considerato – che bisogna guardare più da vicino. Oltre a disposizioni di carattere generale – applicabili a tutti i casi di esternalizzazione, ma con un significato particolare nel campo esaminato – come quelle che impongono un contenuto minimo ai contratti fra banche e fornitori (bene farà, in particolare, l'intermediario a contemplare un'apposita clausola per la «predisposizione di misure di tracciamento idonee a garantire l'*accountability* e la ricostruibilità delle operazioni effettuate, almeno con riferimento alle operazioni critiche e agli

accessi a dati riservati»), il terzo paragrafo è specificamente dedicato al *cloud*.
La Banca d'Italia definisce i servizi *cloud* come «servizi in *outsourcing* erogati secondo modelli innovativi che prevedono la fruizione delle risorse informatiche nella forma di servizi accessibili via rete e configurabili in modo flessibile dall'utente». Dei quattro *deployment models* sopra ricordati, l'unico ignorato è l'*hybrid cloud*, mentre emerge piena padronanza delle infrastrutture *community*, *public* e *private*; quest'ultima semplicemente richiamata, e non anche disciplinata, sulla scorta della considerazione per cui essa non rientrerebbe nella definizione di servizio esternalizzato, in quanto si utilizzano ambienti interni alla società o al gruppo che permettono la condivisione di risorse ICT tra più aree e realtà aziendali. Giova, però, notare, che anche nella nuvola privata si ripetono taluni problemi del *cloud* propriamente esternalizzante, come l'impossibilità di sapere se vi sia stato accesso non autorizzato ai dati. Quanto alla nuvola comunitaria, si pone l'accento sulla necessità che la condivisione delle risorse sia ristretta alle organizzazioni che condividono analoghi necessità e obiettivi. Circa, infine, l'infrastruttura pubblica, si ricorda come, trattandosi di servizi erogati a un vasto numero di utenti con funzionalità offerte in maniera aperta e condivisa, i fornitori di norma sfruttano la possibilità di condividere in modo flessibile le proprie risorse tra i diversi utenti e applicano tariffe *pay-per-use*.
Nel caso dell'acquisizione di servizi in *community* o in *cloud*pubblici i maggiori rischi potenziali possono richiedere una più elevata complessità dei controlli da predisporre, in particolare in caso di esternalizzazione di componenti critiche. A causa della possibilità tecnica per il fornitore di spostare rapidamente e in modo trasparente le risorse dedicate ai vari clienti, è importante che le locazioni dei *data centers* utilizzabili siano preventivamente comunicate. È necessario, in particolare, prevedere adeguati meccanismi di isolamento dei dati di un intermediario rispetto agli altri clienti, a garanzia della loro riservatezza e integrità. Il fornitore è chiamato a garantire contrattualmente il rispetto dei livelli di servizio stabiliti, anche in casi di emergenza o di contesa delle risorse da parte di altri suoi clienti, e ad assicurare la piena ricostruzione degli accessi e delle modifiche effettuate sui dati, anche per finalità ispettive. Sono concordate con il fornitore di servizi modalità di *audit* adeguate alla criticità delle risorse esternalizzate e in considerazione dell'architettura del fornitore.
Venendo, poi, al Garante per la protezione dei dati personali, questi parte dal presupposto che viviamo in «una realtà caratterizzata dalla creatività e dall'inventività dell'uomo, ma che va compresa e regolata affinché l'uomo non ne diventi il prigioniero» [25]. Il primo problema sollevato dal Garante, ma sul punto non si registra unanimità di vedute [26], è che, essendo trattati e conservati su sistemi di *server* dislocati nelle diverse parti del pianeta, i dati sono esposti a numerosi rischi – concretizzati nel *black-out* causato dall'incendio della *server farm* aretina di Aruba nel 2011 – «da quelli sismici a quelli legati a fenomeni di pirateria, non solo informatica» [27]. V'è, poi, il pericolo di perdita o furto di enormi quantità di dati (si pensi, ad es., al *datagate*). Ora, se il possesso dell'immateriale è sempre stato un concetto controverso [28], la perdita del possesso dei dati che si ha con la nuvolaè, si può dire, «di secondo grado»: non solo non si può possedere perché il bene non esiste fisicamente, ma anche il bene immateriale stesso ha, grazie al *cloud computing*, fattezze tali da non consentire alcun esercizio di poteri di fatto. L'evoluzione tecnologica sottrae a qualsivoglia controllo dati e opere dell'ingegno archiviati a migliaia di chilometri di distanza e accessibili solo tramite l'intermediazione di un *internet service provider* (ISP).
Tale è l'importanza della nuvola per la *privacy*, che il Garante, poco dopo l'ampia sezione dedicata ad essa in seno alla citata relazione annuale, ha pubblicato il 1 maggio 2012 il *vademecum* per imprese e P.A.«Cloud computing. *Proteggere i dati per non cadere dalle nuvole*», in cui, oltre a definire il fenomeno nelle sue molteplici sfaccettature ed evidenziarne i rischi, si dedica specifica attenzione al quadro giuridico. Il punto di partenza, difficilmente contestabile, è che «manca ancora un quadro normativo aggiornato 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». Il Garante nutre, in particolare, speranze nel c.d. pacchetto Telecom [29] e nell'approvazione, prevista per il 2014, del nuovo Regolamento generale sulla protezione dei dati (prop. reg. n. 11 del 2012) proposto dalla Commissione. Ciò perché esso introdurrà identiche regole in Europa e nei confronti di Stati terzi (con necessaria riscrittura, quindi, anche del d.lgs. n. 196 del 2003, codice della *privacy*), che si ritiene dovrebbe contribuire a rendere meno complesso e rischioso l'utilizzo di servizi *cloud.*
Una delle più importanti innovazioni di questa riforma è l'estensione dell'obbligo di notifica delle violazioni di

sicurezza riguardanti dati personali a tutti i titolari del trattamento dati come, ad es., banche, assicurazioni, A.s.l., enti locali. I soggetti interessati, quindi, saranno informati senza ritardo della perdita o del furto dei loro dati, ciò che è particolarmente rilevante in un ecosistema *cloudified,* in cui è spesso impossibile accorgersi delle violazioni, oltre che reagirvi. Per altro verso, la riforma segnala un rafforzamento del rango occupato dalla *privacy* nell'impianto assiologico europeo, su cui si dirà qualcosa più oltre. Ora, il codice della *privacy* conferisce all'interessato una serie di diritti, fra cui quello di conoscere quali siano i dati che lo riguardano in possesso della P.A. o di un'impresa, per quale motivo siano stati raccolti e come siano elaborati, potendo richiedere una copia intelligibile dei dati personali che lo riguardano, il loro aggiornamento, la rettifica, l'integrazione, nonché il blocco, la cancellazione o la trasformazione in forma anonima di queste informazioni. Se ciò è vero, il *vademecum* ha cura di precisare che «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».

Va, infine, dato atto di un recente parere reso dal Garante su richiesta dell'Agenzia per l'Italia digitale [30], in ordine a uno schema di «*Linee-guida per il* Disaster Recovery *delle pubbliche amministrazioni*» *ex* art. 50-*bis*, comma 3, lett. *b*), c.a.d. In forza di questa disposizione, le P.A. definiscono il piano di *disaster recovery*, che può essere definito come l'insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate. Il Garante, in particolare, si compiace che siano state accolte le proprie indicazioni, già formulate in un precedente parere (par. n. 394 del 2011), e la normativa europea circa che la necessità che la P.A. tenga in considerazione la particolare natura dei servizi *cloud*, con elettivo riguardo alla possibile delocalizzazione delle *server farms*, individuando gli strumenti e le clausole da adottare per soluzioni *cloud* che implichino il trasferimento dei dati. È proprio ad esito dell'attività consultiva del Garante che l'Agenzia ha previsto che il fornitore indichi «con apposita dichiarazione resa in sede contrattuale, l'esatta localizzazione, o le esatte localizzazioni dei dati gestiti» (*Linee guida*, § 6.5).

Il punto è cruciale non solo per i profili già evidenziati attinenti alla duplice perdita del possesso, ma altresì perché l'art. 45 c.a.d. vieta il trasferimento «anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea», qualora «l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato», dovendosi all'uopo valutare anche «le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza». La disposizione, peraltro, tiene conto dei complessi problemi di responsabilità e diritto internazionale privato derivanti dalla prassi per cui l'attività di *outsourcing* viene subappaltata anche più volte, nell'ambito del medesimo servizio, rendendo, così, ardua l'individuazione di chi effettivamente tratti i dati.

È su questo profilo che si appunta la più recente comunicazione della Commissione concernente (anche) il *cloud* [31]**.**Come è noto, in alcuni settori – obbligazioni contrattuali ed extracontrattuali in testa – esistono norme europee uniformi sulla competenza giurisdizionale, sul riconoscimento e l'esecuzione delle sentenze e sul conflitto di leggi. Esse si applicano a problemi internazionalprivatistici interni all'Unione europea. La Commissione ritiene che a livello internazionale, invece, le norme sui conflitti non siano sufficientemente sviluppate, il che conduce a conflitti di leggi che superano i confini unionali. La conclusione è che «tale complessità sul piano internazionale può incidere negativamente sulla crescita, soprattutto nel caso dei servizi internet che sono per natura transfrontalieri, come ad esempio i servizi di *cloud computing*» (§ 78).

Il punto è che non si può occultare il fatto che, in considerazione del progresso tecnologico, non è attuabile l'idea di limitare la circolazione dei dati ai soli Stati membri e la soluzione percorsa dall'Unione e fatta propria dall'Agenzia per l'Italia digitale non può non destare l'attenzione dei civilisti. Sembra si possa parlare al proposito di una sorta di armonizzazione *soft*,per via contrattuale, delle discipline interne sulla protezione dei dati. Il fondamento giuridico è la dec. n. 87 del 2010, relativa alle clausole-tipo per il trasferimento dei dati personali a incaricati del trattamento stabiliti in paesi terzi, a norma della dir. n. 46 del 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi. Preso atto che le legislazioni possono

essere molto diverse nei paesi terzi e non garantire livelli di protezione adeguate, per l'Agenzia si rende necessario agire contrattualmente, applicando delle clausole specifiche elaborate dalla Commissione Europea, nei contratti di fornitura del servizio. Non potendo esportare, *recta via*, il diritto europeo oltre i consueti confini geografici, si percorre la via solo apparentemente *soft* di fissare standard e preconfezionare clausole. Un'armonizzazione dal basso che può rivelarsi molto più efficace e apparentemente indolore delle forme più tradizionali di ravvicinamento delle legislazioni e garantendo il progresso delle tecnologie dell'informazione e della comunicazione, nella misura in cui agevola l'interoperabilità dei sistemi.
Vale la pena, però, di ulteriormente soffermarsi sul contributo (racchiuso nella richiamate Linee guida) dell'Agenzia per l'Italia digitale, il cui ruolo è veramente cruciale: come dimostra, fra l'altro, la circostanza che essa detiene la *leadership* della fase di progetto di *CloudforEurope* ed è tra i dieci *procurers* di tali servizi, in modalità pre-competitiva. Ora, quantunque le apposite tutele convenzionali previste in detta sede non siano prive di rilevanza, occorre dar atto di almeno due circostanze collegate alla struttura stessa della nuvola informatica. Da una parte, e di ciò è consapevole anche l'Agenzia, i *cloud providers* sono sovente nell'impossibilità di comunicare l'esatta collocazione geografica dei dati gestiti in quanto gli stessi dati sono continuamente movimentati su locazioni diverse, specialmente per evitare rischi di sovraccarico del sistema. Dall'altra, i medesimi dati sono contemporaneamente salvati in molteplici *servers* per prevenire rischi di distruzione. Insomma, l'indicazione dei luoghi fisici di archiviazionerischia di essere uno specchio per le allodole.

3. Il diritto privato europeo fra le nuvole
Il diritto italiano, anche *in subiecta materia*,è evidentemente debitore di quello europeo (basti pensare all'Agenda digitale italiana, non nascostamente attuativa dell'omologa europea) e delle tendenze che si vanno affermando a livello internazionale [32]. Non è un caso che nel momento in cui l'Unione scopre il *cloud computing,* lo inserisce nel più ampio discorso sulla sicurezza informatica e sulla protezione dei dati personali.
Il punto di partenza è la ris. C 321/01 del 2009 [33] su un approccio europeo cooperativo in materia di sicurezza delle reti e dell'informazione, ove si prende atto del fatto che «nuovi sistemi d'uso, quali il *cloud computing* e il *software as a service*, mettono maggiormente in risalto l'importanza della sicurezza delle reti e dell'informazione» (settimo *prendendo atto*). Al profilo securitario si dedica la ris. n. 2009/2229(INI) del 2010 «Governance *di internet: le prossime tappe*», in cui, considerata la nuvolacome un importante aspetto emergente della *governance* di Internet a livello europeo, si invitano la Commissione e gli Stati membri ad intensificare gli sforzi per aumentare la sicurezza del ciberspazio, nonché per partecipare in modo adeguato alla cooperazione internazionale su tale questione, sottolineando la necessità di un approccio multilaterale per fornire una migliore comprensione e consapevolezza sulla competenza in materia di criminalità informatica e di *cloud computing* e l'urgenza di chiarire obblighi e responsabilità di ciascuna delle parti interessate. Nel medesimo solco pure la comunicazione «*Verso una sicurezza informatica mondiale*» (com. n. 163 del 2011). Essa si propone di attuare il piano d'azione «*Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciberattacchi e dalle ciberperturbazioni*» (com. n. 149 del 2009) e a tal fine raccomanda di rafforzare la fiducia nel *cloud computing*.
Venendo all'aspetto della riservatezza, si segnala anzitutto l'articolata com. n. 609 del 2010 su «*Un approccio globale alla protezione dei dati personali nell'Unione europea*». In essa, la Commissione avverte che, sebbene l'attenzione pubblica si concentri sui *social networks,* anche il *cloud computing* costituisce una sfida per la protezione dei dati, in quanto comporta il rischio che l'utente perda il controllo delle informazioni potenzialmente sensibili salvati su programmi ospitati *nell'hardware* di una terza persona (§ 1). La questione si inserisce nel più ampio contesto dello sviluppo tecnologico in un mondo globalizzato, in cui è sempre più frequente il caso di responsabili del trattamento che operano in diversi Stati membri, sottostando così a più giurisdizioni, e che forniscono servizi e assistenza continuativa. Grazie a Internet, i responsabili del trattamento stabiliti al di fuori dello spazio economico europeo possono fornire con maggior facilità servizi a distanza e trattare dati personali in ambienti *online*; inoltre, è spesso difficile localizzare i dati personali e le apparecchiature usate di volta in volta: la nuvolaè l'esempio paradigmatico di questa tendenza e di ciò giuristi e cittadini devono essere ben coscienti (§ 2.2.3).
Detta comunicazione va letta assieme alla ris. n. 2025 del 2011, su un approccio globale alla protezione dei dati

personali nell'Unione europea, la quale invita a chiarire ulteriormente ed a rafforzare le garanzie del trattamento dei dati sensibili e ad una riflessione sulla necessità di trattare nuove categorie, quali i dati genetici e i dati biometrici, in particolare nel contesto degli sviluppi sociali e tecnologici come il *cloud computing*. Il Parlamento europeo rileva, poi, che lo sviluppo e la diffusione della nuvola comportano nuove sfide in termini di tutela della vita privata e protezione dei dati personali e chiede, pertanto, un chiarimento riguardo alle capacità dei responsabili del trattamento dei dati, degli incaricati del trattamento e degli *host*, ai fini di una migliore ripartizione delle rispettive responsabilità giuridiche e affinché gli interessati sappiano dove sono archiviati i loro dati, chi vi ha accesso, chi decide del loro utilizzo e quali procedure di *back-up* e recupero vengono utilizzate. Infine, si invita la Commissione a tenere debitamente conto, in sede di revisione della dir. n. 46 del 1995, le problematiche attinenti alla protezione dei dati in riferimento al *cloud computing* ed a garantire che le norme in materia di protezione dei dati siano applicate a tutte le parti interessate, compresi gli operatori delle telecomunicazioni e di settori diversi dalle telecomunicazioni.

Non si può, poi, trascurare la com. n. 9 del 2012, intitolata «Salvaguardare la *privacy* in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo». Occorre essere consapevoli che, nel contesto della globalizzazione, i dati personali sono trasferiti attraverso un numero crescente di frontiere virtuali e geografiche e conservati su *server* ubicati in più paesi. Un numero crescente di società informatiche offrono servizi *cloud* e ciò impone – al fine di assicurare un'elevata protezione dei dati nei trattamenti internazionali e facilitare la circolazione dei dati oltre frontiera – di migliorare gli attuali meccanismi di trasferimento di dati verso paesi terzi, con decisioni che certificano che le norme sulla protezione dei dati di un paese terzo sono "adeguate", nonché con garanzie appropriate, quali clausole contrattuali tipo o norme vincolanti d'impresa [34]. Ciò posto, la Commissione propone l'adozione di una serie di misure, che, per quanto d'interesse, si sostanziano nell'agevolare i flussi legali di dati verso i paesi terzi grazie al rafforzamento e alla semplificazione delle norme relative ai trasferimenti internazionali di dati verso paesi non oggetto di decisioni di adeguatezza; ciò avverrà, in particolare, razionalizzando e estendendo il ricorso a strumenti quali, appunto, le norme vincolanti d'impresa, in modo che possano essere applicati ai responsabili del trattamento, nonché all'interno dei gruppi di imprese, tenendo così conto del numero crescente di società che effettuano attività di trattamento dei dati, in particolare nel settore del *cloud computing*.

Il *cloud computing* ha ormai raggiunto una tale importanza da costituire l'oggetto esclusivo di un'articolata comunicazione della Commissione denominata «Sfruttare il potenziale del *cloud computing* in Europa» [35]. Al fine di trasformare in atto detto potenziale, è stata condotta, consultando tutti i principali *stakeholders*, un'ampia analisi delle attuali *policies*, discipline giuridiche ed evoluzioni tecnologiche in materia. La finalità, giova precisarlo, non è la creazione di un *cloud* europeo nel senso di infrastruttura *hardware* destinata a fornire servizi generici di nuvola informatica agli utenti del settore pubblico europeo: si vuole mettere a disposizione del pubblico un'offerta in linea con gli standard europei sotto il profilo normativo, ma anche in termini di competitività, apertura e sicurezza. La Commissione, in particolare, dopo aver descritto caratteristiche e vantaggi della nuova tecnologia e aver collocato il discorso all'interno dell'Agenda digitale europea [36], enuclea – oltre a interventi strategici di incentivazione e dialogo internazionale – tre azioni fondamentali che l'Unione si impegna a portare avanti in materia: *a*) predisporre un *corpus* normativo organico e chiaro; *b*) conferire certezza ed equità alle clausole dei contratti coi *provider* di servizi *cloud*; *c*) promuovere un partenariato europeo per il *cloud computing*, sfruttando il ruolo dell'UE di «maggior acquirente mondiale di servizi IT [ciò che le può consentire di] fissare requisiti rigorosi in materia di caratteristiche, efficienza, sicurezza, interoperabilità e portabilità dei dati, come pure in materia di conformità ai requisiti tecnici e può anche stabilire requisiti in materia di certificazione» (§ 3.5, com. n. 529 del 2012). Dalla realizzazione di queste azioni fondamentali la Commissione si attende che «si costituiranno le fondamenta per far sì che l'Europa possa diventare un vero e proprio polo mondiale del *cloud computing*» (§ 5, com. n. 529 del 2012).

Ora, da uno sguardo d'assieme alla comunicazione emerge che, nell'ottica del legislatore europeo, la nuvola informatica merita attenzione specialmente per il suo collegamento con la sicurezza dei dati e la disciplina della compravendita, ambiti che vedono in corso importanti tentativi di armonizzazione. E, d'altronde, anche cercar riparo per via convenzionale è una strada spesso impervia. Ciò poiché quelli in esame, in considerazione della

complessità tecnica della nuvolae del mercato oligopolistico del *cloud providing,* sono contratti con asimmetria di potere contrattuale, per cui il *private enforcement* della protezione dei dati si scontra con la circostanza che anche «organizzazioni grandi hanno uno scarso potere negoziale e spesso i contratti non prevedono clausole di responsabilità quanto all'integrità dei dati, alla riservatezza o alla continuità del servizio» (§ 3.4, com. n. 529 del 2012).
Alla comunicazione in parola sono seguiti – oltre ad una vivace attività consultiva del Garante europeo della protezione dei dati sulla comunicazione della Commissione, del Comitato economico e sociale europeo e del Comitato delle regioni – alcune misure di attuazione, come ad es. la dec. n. C 174/04 del 2013, sulla cui base sono stati costituiti alcuni gruppi di esperti, al fine precipuo di «individuare clausole contrattuali sicure ed eque per i servizi di *cloud computing*, sulla base di uno strumento facoltativo» [37].
Può essere interessante ulteriormente notare come normalmente si pensi che lo sforzo sistematico di edificazione del quadro giuridico in materia sia interesse esclusivo delle parti contrattuali deboli: la Commissione rileva, invece, che «i fornitori di servizi di *cloud computing* hanno indicato che la complessità e l'incertezza del quadro giuridico esistente rendono più difficili le attività transfrontaliere» (secondo *considerando*, dec. 2013/C 174/04). Il miglioramento della qualità dei contratti *cloud* è considerato essenziale al fine di assicurare l'applicazione anche in questo campo della direttiva sulla protezione dei dati personali e, ovviamente, «costruire la fiducia e promuovere la diffusione e lo sviluppo dei servizi di *cloud computing* nell'Unione, tenuto conto del loro notevole potenziale economico» (quarto *considerando*, dec. 2013/C 174/04).
Mentre quello citato è un gruppo di esperti incaricato di occuparsi del contratti *business to consumer* (b2c), per quelli *Business to business* (B2b) il Select Industry Group (SIG), istituito dal Directorate-General for Communications Networks, Content and Technology, Software and Services della Commissione e composto dai rappresentanti delle maggiori società e organizzazioni europee e multinazionali implicate nel *cloud computing*. Il terzo dei sottogruppi del SIG, per quanto qui più direttamente interessa, si fonda sull'impegno della Commissione europea, preso nella comunicazione quadro, a collaborare con esponenti del settore per individuare un codice di condotta per i *cloud providers*, che agevolerà un'applicazione uniforme delle norme sulla protezione dei dati e che è destinato all'approvazione del gruppo di lavoro «Articolo 29» [38] al fine di garantire la certezza del diritto e la coerenza tra il codice di condotta e il diritto eurunionista.
Tornando, poi, agli atti giuridicamente vincolanti e completando la rassegna legislativa con le ultime novità, si segnala il reg. n. 859 del 2013, mirante a realizzare un censimento sullo stato di avanzamento della società europea dell'informazione. Per la prima volta, ci si avvede che un'indagine sulla *information society* che non tenesse conto del *cloud* sarebbe, se non altro, monca. I quesiti connessi alla nuvola cui le imprese saranno chiamate a rispondere sono molteplici, ma, per quanto qui più direttamente interessa, va detto che, come fattori che limitano l'uso dei servizi di *cloud computing,* vengono individuati il rischio di violazioni della sicurezza, i problemi di accesso ai dati o al *software* e l'incertezza circa l'ubicazione dei dati. Tutti profili rispetto al quale i giuristi possono svolgere un ruolo di primo piano.
Ha una genesi agevolmente individuabile, poi, la comunicazione finalizzata a «*Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*»(com. n. 846 del 2013). Dopo il c.d. *datagate*, infatti, l'Unione europea ha sentito la necessità di prendere alcune iniziative per rassicurare i propri cittadini, sfociate, a febbraio 2014, nell'accordo col Brasile per un cavo sottomarino che veicolerà le telecomunicazioni fra i due continenti in totale sicurezza [39]. Per quanto qui più direttamente interessa, invece, l'Unione, esprimendo profonde preoccupazioni per gli abusi dell'*intelligence* statunitense, stigmatizza l'accaduto considerando inaccettabile un controllo di massa delle comunicazioni private, siano esse di cittadini, di imprese o di dirigenti politici. La reazione, però, non può essere di chiusura. Infatti, i trasferimenti di dati personali sono un importante elemento delle relazioni transatlantiche e fanno parte integrante degli scambi commerciali fra le due sponde dell'Oceano, «anche per i nuovi settori emergenti del digitale come i media sociali o il *cloud computing*, che vedono grosse quantità di dati viaggiare dall'Unione europea agli Stati Uniti, e costituiscono anche una componente essenziale della cooperazione fra l'UE e gli USA nel campo delle attività di contrasto della criminalità, e della cooperazione fra gli Stati membri e gli USA nel settore della sicurezza nazionale» (§ 1, com. n. 846 del 2013).
Il riferimento alla nuvola nella comunicazione esaminata non è solo dovuto al momento fortunato vissuto dalla

nuova tecnologia, il rinvio alla quale potrebbe avere il senso di una mera sineddoche retorica. La Commissione, infatti, informa che i programmi statunitensi di *intelligence*«vanno anche a toccare i dati immagazzinati nella nuvola» (*ibidem*). Non manca, poi, l'esplicita critica al *Patriot Act* del 2001, riaffermando che la riservatezza è più importante anche della sicurezza, la quale riveste un altissimo ruolo nella gerarchia dei valori europei. La legislazione richiamata, infatti, consente alle autorità americane di chiedere direttamente alle imprese l'accesso a dati conservati nell'Unione. Pertanto, le imprese aventi sede in Europa possono vedersi chiedere di trasferire dati negli Stati Uniti in violazione del diritto eurunionista e degli Stati membri. È significativo che la preoccupazione della Commissione è che «l'incertezza del diritto che deriva da tali richieste dirette può ostacolare lo sviluppo di nuovi servizi digitali, come il *cloud computing*, che permettono di offrire soluzioni efficaci ed economiche per i cittadini e per le imprese» (§ 2, com. n. 846 del 2013).
Ora, è vero che la riforma della protezione dei dati personali proposta dalla Commissione (accanto alla citata proposta di regolamento, v. la prop. dir. n. 10 del 2012) [40] non prevede nulla di specificamente destinato alla nuvola, ma non è men vero che la prop. reg. n. 11 del 2012 contempla chiare norme «sugli obblighi e le responsabilità degli incaricati del trattamento, come i fornitori di *cloud computing*, anche per quanto riguarda la sicurezza» (§ 3.1, com. n. 846 del 2013). Le imprese che forniscono spazio di archiviazione, e a cui si chiede di fornire dati personali ad autorità straniere, non potranno, quindi, sfuggire alla loro responsabilità invocando il loro *status* di incaricato del trattamento anziché di responsabile del trattamento. Per restituire la fiducia ai cittadini europei (nella sicurezza delle comunicazioni e, quindi, nel *cloud*), conclusivamente, da una parte si auspica una rapida approvazione della riforma della protezione dei dati personali, dall'altra occorre che gli accordi esistenti e futuri garantiscano la continuità di un elevato livello di protezione oltre Atlantico.
La produzione normativa che lega la nuvola alla protezione dei dati non è, però, integralmente fondata, come quella sinora esaminata, sul non confessato presupposto che il *cloud* sia una tecnologia insicura. Esemplare di un approccio diverso è la ris. 18 aprile 2012 sulla relazione annuale sui diritti umani nel mondo nel 2010 e la politica dell'Unione europea in materia, comprese le conseguenze per la politica strategica dell'UE in materia di diritti umani. Ora, non è peregrino ipotizzare che si stia vivendo un vero e proprio «*digital feudalism*» [41], che vede nel *digital divide* solo l'ultima epifania. Ad esso contribuiscono, fra l'altro, la sostanziale negazione del diritto all'accesso Internet (ad onta delle solenni proclamazioni circa una sua presunta fondamentalità) e la mancanza di un'adeguata formazione culturale circa le nuove tecnologie, ciò che di fatto emargina larghe fette specie del sud del mondo. In questo contesto, il Parlamento europeo osserva che le nuove tecnologie possono consentire ai testimoni e ai difensori dei diritti umani di raccogliere informazioni e di condividere la documentazione relativa agli abusi dei diritti umani, elementi che potrebbero essere utilizzati in seguito per assicurare giustizia alle vittime. Esso, inoltre, accoglie con favore le iniziative che prevedono la partecipazione di più soggetti interessati e i codici di condotta come la *Global Network Initiative* e rileva, nondimeno, che il controllo democratico e la difesa dei diritti fondamentali costituiscono compiti essenziali dei governi.
Ciò che qui, però, più direttamente interessa è la convinzione che i difensori dei diritti umani possano rivestire un ruolo più incisivo attraverso «meccanismi sicuri per la raccolta, la cifratura e la memorizzazione di questo tipo di dati sensibili e l'uso di tecnologie *cloud* per garantire che questi dati non vengano scoperti o cancellati» (§ 126). Abbandonare tacite paure e presentare la nuvola come il custode della sicurezza dei dati può davvero contribuire a liberare il potenziale del *cloud* nell'Unione e negli Stati membri.

4. Osservazioni conclusive.
Come si è visto, il principale freno all'espansione della tecnologia in esame è legato ai rischi temuti per laprotezione dei dati.
Questo profilo non è sfuggito a parte della dottrina [42] e si ricollega, anzitutto, al fatto che i file salvati su *cloud* – spesso opere dell'ingegno – possono essere venduti illegalmente o comunque condivisi con soggetti non autorizzati, senza che il titolare ne abbia contezza alcuna. Non è un caso che, come ha evidenziato una ricerca commissionata da IBM, «*77 per cent of respondents believe that adopting cloud computing makes protecting privacy more difficult, while 50 per cent are concerned about data breaches or loss*»[43].
Quanto alla violazione indisturbata dei dati nella nuvola informatica, gli informatici [44] hanno preso atto che nei

sistemi *cloud*, l'utente non è in grado di avvedersi se soggetti terzi stiano facendo uso dei propri dati senza autorizzazione. Peraltro, anche qualora ci si accorgesse dell'uso non autorizzato dei propri beni immateriali, risulterebbe nei fatti impossibile reagire alle violazioni. Ciò dipende primariamente dalla circostanza che tramite il *web-storage* i dati sono gestiti da poche e gigantesche società, quali Apple, Microsoft e Google, che hanno sede di norma negli Stati Uniti, di talché specialmente «*for non-U.S. users the trial is going to be really expensive and so almost impossible for 'normal' users*» [45]. Non si dimentichi che si tratta di contratti tipicamente «alieni» [46] e ad asimmetria di potere contrattuale, in cui vengono imposte unilateralmente pressoché tutte le clausole, compresa la legge applicabile ed il foro competente [47]. Insomma, le complesse questioni di diritto internazionale privato sono solo parzialmente superabili grazie alla disciplina consumeristica, ove applicabile.
Dallo studio della legislazione europea, della contrattualistica e della letteratura in materia di *cloud* emerge la conferma di quanto già dimostrato dalle note vicende della responsabilità degli *internet service providers* (ISP) [48] e dall'abbandono dell'*Anti-Counterfeiting Trade Act* (ACTA), dovuto soprattutto al fatto che non garantiva «il giusto equilibrio tra protezione della *privacy* e responsabilità dei *providers*» [49], com'era stato per gli omologhi statunitensi SOPA [50] e PIPA [51]. Emerge, insomma, la menzionata primazia della riservatezza (e della sicurezza dei dati) nelle gerarchie assiologiche contemporanee.
Il tema qui affrontato impone, infine, una più generale riflessione sui rapporti fra diritto e tecnologia. Qui solo qualche spunto. Chi scrive ritiene che la relazione evocata non riesca a sfuggire dai caratteri dei fenomeni d'isteresi. Il diritto, insomma, reagisce sistematicamente in ritardo alla sollecitazioni proveniente dalla tecnologia, in una rincorsa che non riuscirà mai a colmare uno scarto che si rinnova ciclicamente. Basti pensare, ad es., alla severa repressione della trasmissione in *streaming* di eventi sportivi mediantesiti stranieri [52]: essa ha creato un nuovo mercato per le *apps* che consentono di bypassare i controlli offuscando gli indirizzi IP e navigando in piena riservatezza [53]. Così, si sta provando a rispondere alle sfide del progresso non più col diritto, ma con la tecnologia stessa. In materia di *cloud*, ad es., si stanno sviluppando tecniche crittografiche come la cifratura omomorfica [54] che dovrebbero consentire di esser certi che nessuno possa accedere ai dati esternalizzati, ma si tratta di studi ancora lontani da un approdo stabile. E il paragone col *digital rights management* sembra fornisca elementi che impongono un certo scetticismo circa le possibilità per le misure tecniche di impedire manovre *lato sensu* contraffattorie. Si pensi ai congegni inseriti nei CD musicali per impedirne la duplicazione. Essi,lungi dal raggiungere lo scopo prefissato, hanno contribuito – col parallelo diffondersi di programmi sul modello di Napster – alla crisi dell'industria discografica e alla crescita di mercati digitali basati sulla condivisione. E ora che, grazie a sistemi quali la scansione e stampa tridimensionale [55], l'*openness* è transitata dall'immateriale all'*hardware*,non si può non prendere atto della circostanza per cui nessuna misura tecnologica potrà impedire a un *maker* [56] nel suo *fablab* [57] di riprodurre a piacimento qualsivoglia oggetto, quantunque coperto da IPRs.
Concludendo, nonostante la dimostrata rilevanza del *cloud,* è stato notato che «i legislatori e le istituzioni sono ancora confusi su ciò che [*scil.* la nuvola informatica] realmente può significare per la società dell'informazione» [58]: i giuristi sono quindi chiamati al compito improcrastinabile di (ri)costruire un *framework* normativo adeguato alle nuove sfide, tale da resistere al «*digital tsunami*» [59], non rinunciando a preservare la coerenza del sistema.
Come si è visto, il principale freno all'espansione della tecnologia in esame è legato ai rischi temuti per laprotezione dei dati.
Questo profilo non è sfuggito a parte della dottrina [42] e si ricollega, anzitutto, al fatto che i file salvati su *cloud* – spesso opere dell'ingegno – possono essere venduti illegalmente o comunque condivisi con soggetti non autorizzati, senza che il titolare ne abbia contezza alcuna. Non è un caso che, come ha evidenziato una ricerca commissionata da IBM, «*77 per cent of respondents believe that adopting cloud computing makes protecting privacy more difficult, while 50 per cent are concerned about data breaches or loss*»[43].
Quanto alla violazione indisturbata dei dati nella nuvola informatica, gli informatici [44] hanno preso atto che nei sistemi *cloud*, l'utente non è in grado di avvedersi se soggetti terzi stiano facendo uso dei propri dati senza autorizzazione. Peraltro, anche qualora ci si accorgesse dell'uso non autorizzato dei propri beni immateriali, risulterebbe nei fatti impossibile reagire alle violazioni. Ciò dipende primariamente dalla circostanza che tramite il *web-storage* i dati sono gestiti da poche e gigantesche società, quali Apple, Microsoft e Google, che hanno sede di norma negli Stati Uniti, di talché specialmente «*for non-U.S. users the trial is going to be really expensive and so*

almost impossible for 'normal' users» [45]. Non si dimentichi che si tratta di contratti tipicamente «alieni» [46] e ad asimmetria di potere contrattuale, in cui vengono imposte unilateralmente pressoché tutte le clausole, compresa la legge applicabile ed il foro competente [47]. Insomma, le complesse questioni di diritto internazionale privato sono solo parzialmente superabili grazie alla disciplina consumeristica, ove applicabile.
Dallo studio della legislazione europea, della contrattualistica e della letteratura in materia di *cloud* emerge la conferma di quanto già dimostrato dalle note vicende della responsabilità degli *internet service providers* (ISP) [48] e dall'abbandono dell'*Anti-Counterfeiting Trade Act* (ACTA), dovuto soprattutto al fatto che non garantiva «il giusto equilibrio tra protezione della *privacy* e responsabilità dei *providers*» [49], com'era stato per gli omologhi statunitensi SOPA [50] e PIPA [51]. Emerge, insomma, la menzionata primazia della riservatezza (e della sicurezza dei dati) nelle gerarchie assiologiche contemporanee.
Il tema qui affrontato impone, infine, una più generale riflessione sui rapporti fra diritto e tecnologia. Qui solo qualche spunto. Chi scrive ritiene che la relazione evocata non riesca a sfuggire dai caratteri dei fenomeni d'isteresi. Il diritto, insomma, reagisce sistematicamente in ritardo alla sollecitazioni proveniente dalla tecnologia, in una rincorsa che non riuscirà mai a colmare uno scarto che si rinnova ciclicamente. Basti pensare, ad es., alla severa repressione della trasmissione in *streaming* di eventi sportivi mediantesiti stranieri [52]: essa ha creato un nuovo mercato per le *apps* che consentono di bypassare i controlli offuscando gli indirizzi IP e navigando in piena riservatezza [53]. Così, si sta provando a rispondere alle sfide del progresso non più col diritto, ma con la tecnologia stessa. In materia di *cloud*, ad es., si stanno sviluppando tecniche crittografiche come la cifratura omomorfica [54] che dovrebbero consentire di esser certi che nessuno possa accedere ai dati esternalizzati, ma si tratta di studi ancora lontani da un approdo stabile. E il paragone col *digital rights management* sembra fornisca elementi che impongono un certo scetticismo circa le possibilità per le misure tecniche di impedire manovre *lato sensu* contraffattorie. Si pensi ai congegni inseriti nei CD musicali per impedirne la duplicazione. Essi,lungi dal raggiungere lo scopo prefissato, hanno contribuito – col parallelo diffondersi di programmi sul modello di Napster – alla crisi dell'industria discografica e alla crescita di mercati digitali basati sulla condivisione. E ora che, grazie a sistemi quali la scansione e stampa tridimensionale [55], l'*openness* è transitata dall'immateriale all'*hardware*,non si può non prendere atto della circostanza per cui nessuna misura tecnologica potrà impedire a un *maker* [56] nel suo *fablab* [57] di riprodurre a piacimento qualsivoglia oggetto, quantunque coperto da IPRs.
Concludendo, nonostante la dimostrata rilevanza del *cloud,* è stato notato che «i legislatori e le istituzioni sono ancora confusi su ciò che [*scil.* la nuvola informatica] realmente può significare per la società dell'informazione» [58]: i giuristi sono quindi chiamati al compito improcrastinabile di (ri)costruire un *framework* normativo adeguato alle nuove sfide, tale da resistere al «*digital tsunami*» [59], non rinunciando a preservare la coerenza del sistema.

[1] Com. n. 529 del 2012, «*Sfruttareil potenziale del* cloud computing *in Europa*», § 1.
[2] AA.VV., *Il cielo delle 'nuvole' italiane si tinge d'azzurro*, Ricerca di HP e Politecnico di Milano, Milano, 13-2-2014, inedita.
[3] S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 319-320.
[4] S. RODOTÀ, *ivi*, 321.
[5] L. SCHUBERT-K. JEFFERY (a cura di), *Advances in Clouds. Research in Future Cloud Computing*, Commission of the European Communities, Information Society & Media Directorate-General, Software & Service Architectures, Infrastructures and Engineering Unit, 2012, in cordis.europa.eu, 7
[6] M.R. NELSON, *Building an Open Cloud*, Science, 26-6-2009, 1656, *contra* R. STALLMAN, *Cloud computing is a trap*, 29-9-2008, in *theguardian.com*.
[7] J. MANYIKA et al., *Disruptive technologies: Advances that will transform life, business, and the global economy*, maggio 2013, in *www.mckinsey.com*.
[8] V. spec. i lavori di V. KUMAR-G. RAHEJA-J. SODHI, *Cloud Computing*, in *International Journal of Computers & Technology*, 2013, I, 5 e N. ROBINSON et al., *The Cloud. Understanding the Security, Privacy and Trust Challenges*, Santa Monica, 2011.
[9] L. SCHUBERT-K. JEFFERY (a cura di), *Advances in Clouds*, cit., 71.
[10] Cfr. G. COLANGELO, *L'*enforcement *del diritto d'autore nei servizi* cloud, in *Dir. aut.*, 2012, II, 174; A. MANTELERO, *Il contratto per l'erogazione alle imprese di servizi di* cloud computing, in *Contr. impr.*,2012, IV-V, 1216; A. MANTELERO, *Processi di* outsourcing *informatico e* cloud computing*: la gestione dei dati personali ed aziendali*, in *Dir. inf.*, 2010, 673; G. TROIANO, *Profili civili e penali del* cloud computing *nell'ordinamento giuridico nazionale: alla ricerca di un equilibrio tra diritti dell'utente e doveri dei fornitore*, in *Ciberspazio dir.*, 2011, III, 233; D. LAMETTI,Cloud computing*: verso un terzo* Enclosure Movement*?*, in *Riv. crit. dir. priv.*, 2012, III, 363; S. POIER, *As blurred as a cloud. Preliminary notes questioning some social-legal aspects of cloud computing*, in *Ciberspazio dir.*, 2010, 319.
[11] G. COLANGELO, *L'*enforcement *del diritto d'autore*, cit., 174.
[12] P. LANOIS, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, in *Nw. J. Tech. & Intell. Prop.*, 2010, IX, 29.
[13] Su quest'ultimo aspetto ha posto l'accento la dottrina maggioritaria. V., ad es., T. PETERSON, *Cloudy With a Chance of Waiver: How Cloud Computing Complicates the Attorney-Client Privilege*, in *J. Marshall L. Rev.*, 2012, XLVI, 383; H.B. DIXON jr., *Cloud Computing*, in *The Judges' journal*, 2012, II, 36; M. DANIELE, *Il diritto al preavviso della difesa nelle indagini informatiche*, in *Cass. pen.*, 2012, II, 442, nt. 9; B. CENTRONE, *Il valore è nei dati*, in *Il Sole 24 Ore*, 9-4-2013, 18; L. SCHUBERT-K. JEFFERY (a cura di), *Advances in Clouds*, cit., 2.
[14] M.R. NELSON, *Building an Open Cloud*, cit., 1656.
[15] E. SCHMIDT, Don't Bet Against the Internet, in The Economist, 16-11-2006.
[16] G. COLANGELO, *L'*enforcement *del diritto d'autore*, cit., 176. I casi citati sono A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001) e Metro Goldwin Mayer Studios v. Grokster, 545 US 913 (2005).
[17] A. BENLIAN-T. HESS,-P. BUXMANN (a cura di), Software-As-a-Service: Anbieterstrategien, Kundenbedürfnisse und Wertschöpfungsstrukturen, Wiesbaden, 2010.
[18] G. LAWTON, Developing Software Online With Platform-as-a-Service Technology, in Computer, 2008, VI, 13.
[19] S. BHARDWAJ-L. JAIN-S. JAIN, Cloud Computing: A Study of Infrastructure as a Service (IaaS), in International Journal of Engineering and Information Technology, 2010, I, 62.
[20] Cfr. P. RAJ, Cloud Enterprise Architecture, Boca Raton, 2013, 231; R.L. KRUTZ-R.D. VINES, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Hoboken, 2010, 44; P. MELL-T. GRANCE, The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-145, 2011, in *csrc.nist.gov*, 2.
[21] AA.VV., *CIO Survey*,2013, in *www.netconsulting.it.*
[22] M. FARKAS, *Technology: In Practice: From Desktop to Cloud Top*, in *American Libraries*, 2009, IV, 27.
[23] AA.VV., *Google apre i suoi brevetti al* software *libero*, 29-3-2013, in *www.uibm.gov.it*.
[24] Cfr. A. NIGRO, *La nuova normativa sulla trasparenza*, in *Dir. banca merc. fin.*, 1993, 575; U.M. GIORDANO, *La trasparenza delle condizioni contrattuali nella nuova legge bancaria*, in *Riv. soc.*, 1993, 1254; G. ROSSI, Antitrust *e teoria*

della giustizia, in *Riv. soc.*, 1995, 13; G. DI CHIO, *Gli intermediari: il sistema di vigilanza e l'esercizio dei servizi di investiment*, in *Società*, 1998, V, 502; J. BASEDOW, *The States Private Law and the Economy. Commercial Law as an Amalgam of Public and Private Rule-Making*, in *American Comparative Law Journal*, 2008, III, 703 e, pur con accezioni non sovrapponibili, S. CASSESE, *Il diritto amministrativo: storie e prospettive*, Milano, 2010, 530 e T. ASCARELLI, *Appunti di diritto commerciale*, 2ª ed., Roma, 1933, 17.
[25] F. PIZZETTI, *Uomini e dati. Evoluzione tecnologica e diritto alla riservatezza*, in *Foro it.*, 2011, IX, 5, 230.
[26] E.A. BERTRAM, *How to Keep Your Invention Patentable While It Is Stored in the Cloud: A Guide for Small Inventors,* in *Fed. Cir. B.J.*,2011-2012, XXI, 389.
[27] F. PIZZETTI, *Uomini e dati*, cit., 237.
[28] Cfr. T. JEFFERSON, *To Mr Isaac M'Pherson,* Monticello, 13-8-1813, in WASHINGTON (a cura di), *The Writings of Thomas Jefferson*, VI, Washington D.C., 1854, 180; M. PLANIOL, *Traité élémentaire de droit civil*, I, Paris, 1900, 455; S. PUGLIATTI, *La proprietà e le proprietà (con riguardo particolare alla proprietà terriera)*, Atti del terzo congresso nazionale di diritto agrario, Palermo, 19/23-10-1942, Milano, 1954, ora in *La proprietà nel nuovo diritto*, Milano, 1964, 249.
[29] V. le dir. nn. 19, 20, 21, 22, 58 del 2002, con le novità introdotte dalla dir. n. 140 del 2009 e dai reg. n. 144 del 2009 e n. 717 del 2007.
[30] GPDP, par. n. 333 del 2013.
[31] Com. n. 72 del 2014, «Governance *e politica di internet. Il ruolo dell'Europa nel forgiare il futuro della* governance *di internet*».
[32] V. gli atti della XXXIVª *Conferencia Internacional de Autoridades de Protecciòn de Datos y Privacidad*, il cui esito è stato una *Resolution on Cloud Computing*.
[33] Questa risoluzione è del Consiglio, a differenza delle altre qui citate, che sono del Parlamento europeo.
[34] Si tratta di codici di pratiche basate sulle norme europee per la protezione dei dati, approvati da almeno un'autorità di protezione dei dati, che le organizzazioni elaborano su base volontaria e applicano per assicurare adeguate garanzie di sicurezza per le categorie di trasferimenti di dati personali tra imprese che sono parte dello stesso gruppo di società, e che sono vincolate da tali norme.
[35] Com. n. 529 del 2012, nel prosieguo anche "comunicazione quadro".
[36] V. spec. i §§ 2.5.1 e 2.5.3, com. n. 245 del 2010 e la ris. n. 2009/2225(INI) del 2010.
[37] Comm. eur., comunicato n. IP/13/990 del 2013.
[38] Si tratta del «Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali» di cui all'art. 29, dir. 1995/46, formato dai Garanti della *privacy* nazionali ed europeo.
[39] *Joint Statement* n.6930 del 2014, VII *summit* UE-Brasile, Bruxelles, 24 febbraio 2014.
[40] V., da ultimo, A. MANTELERO, *La riforma della data protection in Europa: un'opportunità per le imprese*, in *Giustiziacivile.com*, 3 marzo 2014.
[41] S. MEINRATH-J. LOSEY-V. PICKARD, *Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide*, in *CommLaw Conspectus*, 2011, 423.
[42] V., in particolare, M. SOFFIENTINI,Cloud computing *e* privacy, in *Dir. prat. lav.*, 2013, XLII, 2465; W.K. HON-C. MILLARD-I. WALDEN, *The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1*, Queen Mary School of Law Legal Studies Research Paper No. 75/2011, in *International Data Privacy Law,* 2011, I, 211; F. PIZZETTI, *Uomini e dati*, cit., 237; A. MANTELERO, *Processi*, cit., 673; C. SOGHOIAN, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, in *J. on Telecomm. and High Tech. L.*, 2009, VIII, 359 e R.C. PICKER, *Competition and Privacy in Web 2.0 and the Cloud*, U of Chicago Law & Economics, Olin Working Paper No. 414, ssrn.com/abstract=1151985
[43] N. COLEMAN, *Cloud computing Cloud control*, in *Lawyer*, 2011, 35.
[44] B.P. RIMAL-E. CHOI-I. LUMB, *A Taxonomy and Survey of Cloud Computing Systems*, NCM '09 Proceedings of the 2009 Fifth International Joint Conference on INC, IMS and IDC, Washington DC, 2009, 44.
[45] S. POIER, *As blurred as a cloud*, cit., 324.
[46] G. DE NOVA, *Il contratto "alieno"*, in *Riv. dir. priv.*, 2011, IV, 487.
[47] G. MANTELERO, *Il contratto*, cit., 1220.
[48] I riferimenti giurisprudenziali principali sono Corte giust. UE, sez. III, 16 febbraio 2012, C-360/10, *Belgische*

Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV, in *Dir. ind.,* 2012, 346; Corte giust. UE, sez. III, 24 novembre 2011, C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* in *Racc.*, 2011, I-11959

[49] G. COLANGELO, *L'*enforcement *del diritto d'autore*, cit., 142.

[50] Acronimo dello *Stop Online Piracy Act* (H.R. 3261).

[51] Si tratta del *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* (Senate Bill 968 or S. 968).

[52] V., ad es., Trib. Milano, g.i.p., 7-1-2013, inedita, che ha disposto il sequestro preventivo di dieci siti Internet che, fornendo al loro interno dei *link* a siti per lo piu stranieri privi del diritto di esclusiva per la trasmissione sul territorio italiano, permettevano agli utenti italiani di visionare in *streaming* partite di calcio in violazione del diritto d'autore di R.T.I. (Reti Televisive Italiane S.p.a.).

[53] Questi sistemi vanno moltiplicandosi a ritmo serrato e per ogni *app* o sito bloccati, ne nascono almeno altrettanti in grado di soddisfare una domanda crescente. V., a titolo meramente esemplificativo, i sistemi Hola, ProXPN, Tunnelbear, HotSpotShield, VPN Oneclick, Hideman VPN e Tigervpns VPN.

[54] La cifratura omomorfica è una tecnica crittografica grazie alla quale specifici tipi di computazione possono essere portati su *ciphertext* (testo cifrato) e generare un risultato cifrato che, una volta decriptato, corrisponde al risultato delle operazioni poste in essere sul *plaintext* (testo in chiaro). I *puncta dolentes* sono due: da una parte, trovare un bilanciamento fra sicurezza e funzionalità, dall'altra evitare l'effetto tipicamente connesso alle tecniche crittografiche tradizionali, per cui non si può operare sui dati criptati. Cfr., *ex plurimis*, S. RASS-D. SLAMANG, *Cryptography for Security and Privacy in Cloud Computing*, Norwood, 2014; H. RAHMANI-E. SUNDARARAJAN-Z.MD. ALI, *A Homomorphic Scheme in untrusted multi-servers cloud model*, in KRISHNA HARI-TOMAR-SAIKISHORE-KIM (a cura di), *Proceedings of the International Conference on Cloud Computing and eGovernance 2012*, Pondicherry, 2012, 36 e N.P. SMART-F. VERCAUTEREN, *Fully homomorphic encryption with relatively small key and ciphertext sizes*, in NGUYEN-POINTCHEVAL (a cura di), *Public Key Cryptography - PKC 2010*, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, 26/28-5-2010, Berlin-Heidelberg-New York, 2010, 420.

[55] La stampa 3D (anche detta *additive manufacturing* o *rapid prototyping*) permette di avere una riproduzione fisica di un modello 3D realizzato con un software di modellazione 3D, come Autocad. Attraverso l'immissione del disegno, la macchina, seguendo determinate coordinate, riesce a produrre un modello fisico, che spesso è utilizzabile come prodotto finito. Ciò che sta contribuendo alla grande diffusione di questo sistema è lo scanner 3D, che consente di riprodurre qualsiasi oggetto anche se non si sia in gradi di adoperare programmi di modellizzazione. È sufficiente puntare lo scanner contro l'obiettivo desiderato ed esso stesso elabora il progetto da caricare sulla stampante 3D.

[56] Col termine *makers* si designa una generazione di creativi che, grazie soprattutto al *3D printing*, si stanno emancipando dalle grandi fabbriche, riappropriandosi tanto dell'ideazione quanto della stessa realizzazione degli oggetti.

[57] I *fabrication laboratories*, piu conosciuti come *fablabs*, sono piccole officine che offrono servizi personalizzati di fabbricazione digitale, sono stati lanciati dal Medialab del MIT nel 2003 per replicare laboratori dove produrre facilmente oggetti ad alto livello di personalizzazione e qualita, cio che la produzione di massa non sembra poter assicurare. Si assiste alla nascita continua di nuovi *fablabs*, anche in Italia, dove per esempio sono notevoli le esperienze delle Officine Arduino (dal nome di un noto microprocessore *OS* inventato ad Ivrea) di Torino, del 3DiTaly di Roma e del Fablab Palermo, ospitato dall'associazione Spazio Trentasei Archiarte Palermo (v. *http://fablabtorino.org/*; *www.3ditaly.it* e *http://fablabpalermo.org/*) . Si tratta di spazi *open*, in cui i progetti sono condivisi in rete e vengono realizzati con strumenti essi stessi *open*.

[58] G. TROIANO, *Profili civili e penali del* cloud computing,cit., 261.

[59] AA.VV., *Freedom, Security, Privacy – European Home Affairs in an open world*, Report of the Informal High-Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group"), giugno 2008, in *register.consilium.europa.eu*, § 132.