UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DIPARTIMENTO DI GIURISPRUDENZA

DOTTORATO DI RICERCA

IN

DIRITTO DELLE PERSONE, DELLE IMPRESE E DEI MERCATI

XXIX CICLO

TESI DI DOTTORATO

Diritto e "nuvole"

Profili giuridici del *cloud computing*

Coordinatore:

Ch.mo Prof. Enrico Quadri

Tutor:

Ch.ma Prof.ssa Luciana D'Acunto

Dottorando:

dott. Emilio Tucci

Diritto e “nuvole”

Profili giuridici del *cloud computing*

INDICE

Premessa

La diffusione dell'informatica e della telematica è aumentata vertiginosamente così come le occasioni di contatto con le nuove tecnologie, ormai realtà in grado di caratterizzare la moderna società in tutte le sue declinazioni.

Dalla macchina di *Touring* alle più moderne *app*, la tecnologia da strumento *"per"* il diritto è diventata sempre più oggetto *"del"* diritto.

Il giurista, chiamato a confrontarsi con l'innovazione, deve mettere costantemente in discussione concetti acquisiti ed ormai parte del proprio bagaglio culturale. La sicurezza delle relazioni giuridiche può oggi essere raggiunta grazie all'utilizzo della tecnologia digitale che, gradualmente, sta sostituendo i tradizionali strumenti di scrittura ed archiviazione a cui sono saldamente legati la certezza e l'evoluzione del diritto.

L'informatica, infatti, ha fornito nuovi mezzi per rappresentare, trasmettere e conservare il pensiero con la conseguente necessità di nuove regole in grado disciplinarne l'utilizzo. Le richieste sempre crescenti di servizi informatici tesi a soddisfare le esigenze del singolo utente o quelle di *business* delle imprese hanno determinato un incremento costante del numero dei *server* utilizzati nei *data center* con conseguente crescente virtualizzazione della memorizzazione dei dati. Si assiste sempre più ad un utilizzo di *internet* per un'elaborazione centralizzata dei dati ed uno *storage* virtuale degli stessi, con notevoli opportunità per gli utenti in grado di fruirne da remoto, grazie ai grandi *data*

repository ed alla capacità centralizzata di elaborazione dei dati[1] alla base della nuova tecnologia *cloud.* Il *cloud computing (nuvola informatica)*, infatti, può essere sinteticamente inteso *"[...] come l'archiviazione, l'elaborazione e l'uso di dati su computer remoti e il relativo accesso via Internet. In altre parole 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 cloud computing ha tutti i numeri per abbattere i costi sostenuti dagli utenti dei servizi tecnologici e per aprire le porte allo sviluppo di tanti nuovi servizi. Grazie all'uso della nuvola informatica, anche le imprese più piccole possono accedere a mercati sempre più grandi, mentre i governi possono rendere i propri servizi più interessanti contenendo i costi"*[2].

Il *cloud*, in altre parole, consente di spostare i sistemi di archiviazione e di elaborazione dei dati nonchè i servizi di rete verso elaboratori centralizzati prescindendo dai singoli *computer* e dai *server* locali. Nell'era della nuvola informatica, le informazioni e le applicazioni saranno sempre più collocate nel *cyberspazio* piuttosto che nei singoli *device* degli utenti: *"the network will truly be the computer"*[3].

Il successo di soluzioni quali *Dropbox*, *Google Drive*, *iCloud*, *OneDrive*, *etc.*, testimonia la persistente crescita della tecnologia *cloud* che sta segnando

---

[1] Sul punto, *cfr.* C. YOO, *Cloud Computing: Architectural and Policy Implication*, 2011, reperibile su *http://ssrn.com/abstract=1824580*.

[2] Così Comunicazione della Commissione Europea al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Sfruttare il potenziale del cloud computing in Europa*, 27.09.12, COM(2012) 529 final, reperibile su *http://ec.europa.eu /transparency/regdoc/rep/1/2012/IT/1-2012-529-IT-F1-1.Pdf*.

[3] E. SCHMIDT, *Don't be against the Internet*, in *The Economist*, reperibile su *www.economist.com/the worldin/businnes/displayStory.cfm?story_id=8133511&d=2007*.

l'ingresso di *internet* in una nuova dimensione, mutando il modello di creazione, sviluppo, aggiornamento e fruizione delle applicazioni inserite in particolari infrastrutture.

Gli utenti abbandonano ormai costantemente l'utilizzo dei programmi tradizionali (*Office*, *Outlook*, *etc.*) installati sui propri PC optando per soluzioni che utilizzano meccanismi informatici di elaborazione non locali ma centralizzati (*Google Docs*, *Microsoft Office Live*, *Gmail*, *etc.*).

Lo sviluppo del *cloud* è stato sicuramente incentivato dalla diffusione della banda larga e di dispositivi collegati alla rete che consentono – ventiquattro ore su ventiquattro e sette giorni su sette, salvo attività di manutenzione programmata – la cd. accessibilità "*anytime*" e "*anywhere*". La velocità e l'elasticità con cui vengono fornite o rilasciate le risorse per incrementare o decrementare la capacità computazionale costituiscono un altro importante valore aggiunto della tecnologia *cloud* che appare idonea a fornire, in qualsiasi momento, sulla scorta del modello economico "*pay as you go*", risorse illimitate e capacità aggiuntiva. L'utilizzo di applicazioni gestite su infrastrutture remote consente una più facile gestione per i *cloud consumer* garantendo, al contempo, ai *cloud provider* una gestione centralizzata dei servizi offerti ad un numero rilevante di fruitori con la conseguente riduzione dei costi di distribuzione, manutenzione ed aggiornamento, a vantaggio degli stessi *consumer* che potranno beneficiare di prezzi ridotti per l'uso dei sistemi *cloud*.

Gli utenti *cloud*, inoltre, potendo contare su un'ampia offerta di piattaforme, *software* e servizi infrastrutturali *web based* a costi contenuti, non dovranno preoccuparsi dell'infrastruttura tecnologica, ma potranno dirigere altrove i

propri risparmi se consumatori finali o concentrarsi sul proprio *business* per aumentarne la produttività se rientranti nella categoria dei professionisti.

La tecnologia *cloud*, se da un lato consente di ottenere flessibilità, efficienza, ottimizzazione delle risorse e contenimento dei costi, dall'altro presenta anche criticità relative alla qualificazione dei contratti di *cloud*, alla legge applicabile, alla competenza giurisdizionale, alla responsabilità dei *cloud provider* ed alla tutela della *privacy* nei rapporti di *cloud computing*.

In particolare il *cloud computing* è stato analizzato – dopo averne delineato le caratteristiche principali, l'architettura ed i modelli di distribuzione al fine di meglio comprendere le questioni giuridiche d'interesse – sotto il profilo della struttura e della qualificazione del contratto, della standardizzazione delle clausole contrattuali, della tutela del contraente debole e dell'abuso di dipendenza economica nei rapporti B2b.

Non sono stati tralasciati, inoltre, gli aspetti relativi alla tutela della *privacy*; delineato il quadro normativo di riferimento, anche alla luce del nuovissimo Reg. UE 2016/679, ci si è soffermati su ruoli e responsabilità nel trattamento dei dati, misure minime di sicurezza e principio di *accountability*, *standard* ISO per il *cloud* e trasferimento dei dati all'estero.

È stato altresì considerato il profilo della responsabilità extracontrattuale del *cloud provider* da ricondurre alla disciplina dettata dal d.lgs. 70/03 in attuazione della Direttiva 2000/31/CE.

Le riferite questioni sono state affrontate in un'ottica transnazionale considerando che i servizi *cloud*, nella maggior parte dei casi, sono erogati da prestatori localizzati al di fuori dei confini nazionali ed europei.

Capitolo I
La tecnologia *cloud*

SOMMARIO: 1. Le caratteristiche del *cloud computing*; 2. I diversi tipi di *cloud*; 3. I modelli di distribuzione dei servizi *cloud*.

1.- *Le caratteristiche del cloud computing.*

Il primo a parlare pubblicamente di *cloud computing* nel 1961 fu John Mc Carthey in occasione del centenario del *Massachussetts Institute of Technolgy* (MIT). In particolare, l'idea del *time sharing* dei *computer* fu individuata come un'importate opzione di "vendita" della potenza di calcolo dei PC e di specifiche applicazioni secondo il modello economico dell'utilità.

L'*hardware*, il *software* ed il sistema di telecomunicazioni dell'epoca, però, non furono in grado di sostenere questa innovazione che, solo con la crescita di *internet* e l'avvento di *device* e programmi più performanti, ha iniziato ad affermarsi sino ad essere considerata modello di riferimento in grado di incrementare la produttività, la crescita e l'occupazione.

Il *cloud*, infatti, evoluzione dei tradizionali *data center* grazie alla nuova modalità di memorizzazione, archiviazione ed elaborazione dei dati attraverso *hardware* e *software online* a disposizione degli utenti, sta avendo una vertiginosa espansione rendendo competitivi sul mercato globale anche singoli utenti e piccole aziende in grado di disporre di una elevatissima potenza di calcolo con esiguo investimento economico.

La "nuvola", espressione diretta di *internet* unico elemento realmente necessario per il suo funzionamento, è sempre più protagonista con lo sviluppo di risorse di *storage* e *processing* a cui è possibile accedere, da remoto, facendo a meno della memoria del proprio *computer* e di costosi *software* per l'elaborazione dei dati.

Caratteristica fondamentale dei sistemi *cloud* è la loro scalabilità intesa come possibilità di erogare risorse informatiche sulla scorta delle reali esigenze degli utenti consentendo un evidente risparmio di costi scaturente dal mancato impiego di denaro per l'acquisizione della tecnologia ritenuta necessaria a far fronte a tutte le potenziali necessità e poi, di fatto, sottoutilizzata e comunque soggetta alla cd. obsolescenza tecnologica.

L'interazione e l'evoluzione di tecnologie esistenti ha dato origine al *cloud computing* ritenuto oggi in grado di rimodellare l'intera industria dell'IT e definito dal NIST[4] come un modello per *"[...] enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, Three service models, and four deployment models [...]*"[5].

[4] *National Institute of Standards, Information Technology Library*.

[5] Il *cloud computing*, in altre parole, è un modello che permette di ottenere un facile accesso di rete *on demand* ad un gruppo di risorse computazionali configurabili (e.g. reti, *server*, applicazioni e servizi) che possono essere rapidamente allocate e rilasciate con un ridotto impegno di gestione e di interazione con il fornitore del servizio. Il testo completo della definizione elaborata dal NIST può essere reperito all'indirizzo *http://nvlpubs.nist.gov /nistpubs/Legaci /SP/nistspecialpublication800-145.pdf.*

La suddetta definizione consente di rilevare almeno cinque caratteristiche fondamentali del *cloud* così sintetizzabili: *on demand self service*, *broad network access*, *resource pooling*, *rapid elastic*, *mesured service*.

In particolare, infatti, i fruitori del *cloud*, per soddisfare le proprie esigenze, possono utilizzare le risorse necessarie (*hardware*, applicativi e *storage*) senza l'intervento del fornitore del servizio modificando in qualsiasi momento le proprie richieste in virtù del *cd.* modello del *pay for use* (***on demand self service***). L'accesso ai servizi, grazie alla rete *internet*, può avvenire in ogni momento e da qualsiasi luogo con un sistema che consente la piena condivisione dei dati e la collaborazione *online* (***broad network access***). Le risorse messe a disposizione dai *cd. cloud provider*[6] sono condivise ed allocate in modo dinamico da tutti gli utilizzatori grazie alla virtualizzazione ed al modello *multi-tenancy*. L'*hardware* (*hardisk*, CPU, RAM, *etc.*) è invisibile all'utente che, in linea generale, non ne ha il controllo ignorandone il suo esatto posizionamento nel mondo (***resource pooling***). Gli utenti dei servizi *cloud* possono acquisire, in qualsiasi momento, le risorse senza dover pianificare in anticipo il proprio bisogno evitando così anche il fenomeno del sovradimensionamento/sottodimensionamento. Il modello del *pay for use* permette di assecondare la domanda dei *cloud consumer* evitando, come anticipato, sottoutilizzi o sovrautilizzi delle risorse con il conseguente risparmio di costi tarati su utilizzi effettivi (***rapid elastic***). L'infrastuttura *cloud* permette agli utenti il controllo costante delle risorse utilizzate garantendo la

[6] Il *cloud provider* è il fornitore di servizi intesi come server virtuali, *storage*, applicazioni complete, *etc.* secondo il modello del *pay per use*.

possibilità di verificare la rispondenza dei costi sostenuti all'utilizzo effettivo dei servizi (***mesured service***).

Il crescente successo della tecnologia *cloud* è indubbiamente legato al miglioramento della velocità e della qualità della connessione al *web*, elemento imprescindibile per l'utilizzo dei nuovi servizi delocalizzati. I collegamenti mobili a basso costo con tariffe *"flat"* comprensive di discreta quantità di traffico *internet* mensile, la corrispondente diffusione di dispositivi portatili *cloud based* e la capillare diffusione dei *social network*, hanno fornito ulteriore impulso all'affermazione della tecnologia *cloud* con la maggiore consapevolezza per gli utenti che i propri dati non sono fisicamente collocati in un posto preciso.

L'utilizzo della nuvola è cresciuto in modo esponenziale anche in ambito professionale in ragione degli indubbi vantaggi che possono scaturire dalla sua adozione. L'eliminazione o la riduzione dell'infrastruttura IT è in grado di determinare un'importante riduzione di costi per investimenti *hardware* e *software*, licenze, manutenzione, energia elettrica, risorse umane e formazione.

Gli utenti "*business*" potranno disporre di aggiornamenti frequenti dei sistemi remoti senza necessità di interventi sui sistemi locali. L'operatività delle piattaforme *cloud* consente, inoltre, una rapida fruibilità delle risorse senza dover dipendere dai tempi di sviluppo delle soluzioni *software* cd. *"tailor made"*.

La riferita scalabilità del *cloud*, inoltre, consente una rapida rimodulazione dei servizi sottoscritti con la conseguente definizione degli *asset* aziendali sulla base dei reali bisogni di operatività.

L'ubiquità dell'accesso consente la migliore organizzazione del lavoro e la sua ottimizzazione.

Sicuro rilievo ha, infine, la possibilità di esternalizzare i rischi connessi alla gestione dei dati laddove le misure atte a garantire sicurezza ed integrità sono delegate al *cloud provider*.

L'utilizzo delle potenzialità del *cloud* presuppone, in ogni caso, l'adozione di cautele tese ad evitare alcune criticità insite nel nuovo sistema tecnologico.

L'utente deve valutare con particolare attenzione e scrupolosità il contratto e gli strumenti che definiscono caratteristiche e qualità del servizio a garanzia della sicurezza e della riservatezza dei dati. È necessario, inoltre, disporre di una connessione di elevata qualità onde evitare impedimenti per l'accesso ai servizi ed ai dati in *cloud*.

La grande attenzione al fenomeno *cloud*, considerato opportunità di crescita e sviluppo, è dimostrata dal suo costante richiamo da parte del legislatore italiano ed europeo pur in assenza di una definizione normativa[7]. In particolare, il *cloud* è menzionato dal d.l. 5/12[8] come strumento da implementare nell'ambito dell'Agenda digitale italiana, sotto il controllo della cd. cabina di regia, per *"le attività e i servizi delle pubbliche amministrazioni"*. Il Codice dell'amministrazione digitale[9] (CAD) – pur prevedendo i requisiti tecnici che gli archivi informatici, anche *web based*, devono rispettare per essere a norma

[7] Per ben comprendere i profili giuridici connessi all'utilizzo del *cloud*, in assenza di una definizione normativa, è opportuno tenere in considerazione la sua struttura tecnologica ed il relativo funzionamento.
[8] V. art. 47, co. 2 *bis*, d.l. 9 febbraio 2012, n. 5, recante disposizioni urgenti in materia di semplificazione e di sviluppo, convertito con modificazioni dalla l. 4 aprile 2012, n. 35. Il co. 2 bis, art. 47 è stato poi abrogato dall'art. 64, co. 3, d.lgs. 26 agosto 2016, n. 179, a decorrere dal 14 settembre 2016, ai sensi di quanto disposto dall'art. 66, co. 1, dello stesso d.lgs. 179/2016.
[9] D.lgs. 7 marzo 2005 n. 82, Codice dell'amministrazione digitale.

– non qualifica i rapporti contrattuali che si instaurano tra le parti anche laddove una di esse sia un soggetto pubblico.

Il CAD, inoltre, all'art. 68, co. 1, lett. d), richiama esplicitamente il concetto di *cloud* prevedendo che *"le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato: [...] d) software fruibile in modalità cloud computing* […]*"*.

In ambito europeo, il Comitato economico e sociale europeo (CESE) ha evidenziato[10] le caratteristiche principali del nuovo sistema di utilizzo e gestione delle risorse informatiche[11] mentre, come anticipato, la Commissione Europea ha sottolineato[12] che il ricorso ai servizi *cloud* può generare opportunità di crescita per l'economia dell'Unione con particolare riferimento alle piccole medie imprese ed alla pubblica amministrazione rilevando, al contempo, che il principale ostacolo ad una diffusione ancora più capillare del *cloud* è rappresentato dalla frammentazione del quadro normativo di riferimento.

L'utilizzo del *cloud*, sotto un profilo prettamente giuridico, ha determinato il passaggio da un modello basato sulla necessità dell'acquisizione della proprietà di una data tecnologia o, comunque, del diritto di utilizzarla in forza di diversi

[10] *Cfr.* il parere del Comitato economico e sociale europeo in merito a *"Il cloud computing in Europa (parere di iniziativa)"* in GUUE 28 gennaio 2012.
[11] Il CESE ha individuato nella dematerializzazione, nella facilità di accesso, nell'allocazione dinamica delle risorse, nella scalabilità della tecnologia e nella condivisione, le caratteristiche tecniche del *cloud*.
[12] Sul punto, *cfr.* la precedente nota 2.

tipi contrattuali[13], ad un modello basato sull'accesso da remoto ai servizi messi a disposizione dai *cloud provider* con conseguente disponibilità temporanea degli stessi servizi sulla scorta del sistema *pay for use*[14].

La Commissione Europea, con la sua comunicazione, ha sostenuto l'importanza di interventi mirati per accrescere la fiducia nelle soluzioni di *cloud computing* garantendo l'interoperabilità tecnica delle piattaforme *cloud* e la portabilità dei dati[15] nonchè l'interoperabilità giuridica dei contratti alla base dei servizi *cloud* con l'obiettivo della definizione di uno *standard* contrattuale.

2.- *I diversi tipi di cloud.*

I servizi di *cloud computing* sono suddivisi, in base al tipo di risorsa remota, in *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS), *Software as a Service* (SaaS)[16].

L'*Infrastructure as a Service* è la prima categoria di servizi *cloud* ovvero l'offerta di capacità di elaborazione o di memoria a soggetti che vi accedono via *internet*. L'utente, attraverso questo sistema, ha a sua disposizione le potenzialità e la flessibilità di un *computer* senza però doversi preoccupare

---

[13] Si considerino le licenze d'uso di *software*, a titolo gratuito o a titolo oneroso, o anche i contratti di locazione o di *leasing* aventi ad oggetto sistemi informatici.

[14] Per un approfondimento sul modello dell'accesso ai servizi alternativo al modello cd. proprietario v. J. RIFKIN, *L'era dell'accesso. La rivoluzione della new economy*, Milano 2000. Sul tema della cultura economica dell'accesso e del relativo approccio giuridico v. A. STAZI, *"Marketplace of ideas" e "accesso pluralistico" tra petizioni di principio e ius positum*, in *Dir. informazione e informatica*, 2009, 635 ss.

[15] L'interoperabilità finalizzata alla portabilità dei dati è essenziale per evitare il *cd.* fenomeno del *lock in* che si verifica quando l'utente viene a trovarsi in un rapporto di dipendenza con il fornitore di servizi tale da trovarsi nella condizione di non poter rivolgersi ad altro fornitore senza essere disposto a sostenere costi rilevanti per effettuare il passaggio. In altre parole, l'utente resta imprigionato dalla tecnologia scelta in prima battuta poiché il trasferimento ad altro fornitore di servizi, senza i necessari costosi adattamenti tecnici, gli impedirebbe l'utilizzo dei dati creati ed elaborati con il sistema originariamente utilizzato.

[16] Sul punto, *cfr. "the NIST definition of cloud computing"*, reperibile all'indirizzo *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nist specialpublication800-145.pdf*.

dell'*hardware* e della continuità del servizio in caso di guasti. Coloro che usufruiscono di servizi IaaS acquistano risorse *on demand*, il più delle volte tramite *Virtual Machine*[17], da utilizzare sia per fornire servizi IT interni sia per fornire servizi *online* al pubblico.

Il *cloud consumer*, che in questo caso è quasi sempre un'impresa, usufruisce direttamente dell'infrastruttura IT (*processing*, *storage*, *networks* ed altri fondamentali risorse). Tipico esempio di IaaS è il prodotto *Amazon Elastic Compute Cloud* (Amazon EC2) servizio *web* che fornisce capacità di elaborazione informatica nel *cloud* che può essere dimensionata in ragione delle necessità.

L'utente, tramite un'interfaccia *web*, ha la possibilità di configurare il servizio con il controllo completo delle proprie risorse informatiche che possono essere eseguite nell'ambiente di elaborazione di Amazon. Gli sviluppatori con il servizio Amazon EC2 hanno a disposizione tutti gli strumenti per creare applicazioni ed isolare le stesse dagli scenari, più comuni, di errore.

La seconda categoria nota è quella dei servizi PaaS consistenti nell'offerta di un ambiente di sviluppo che permette di creare applicazioni *web* senza installare alcuno strumento sul proprio PC e senza preoccuparsi dell'infrastruttura attraverso cui è stata realizzata la piattaforma di sviluppo.

---

[17] La *Virtual Machine* (VM) è un ambiente virtuale, creato con uno specifico *software*, che emula il comportamento di una macchina fisica attraverso l'associazione di risorse *hardware* (*hard disk*, RAM, *etc.*) ed in cui alcune applicazioni sono eseguite come se interagissero con tale macchina. L'utilizzo della VM consente, tra le altre cose, di poter offrire, contemporaneamente ed in modo efficiente, a diversi utenti, ambienti operativi separati, ciascuno attivabile su effettiva richiesta, senza incidere sul sistema fisico reale con il partizionamento del disco rigido.

Il fornitore del servizio, infatti, fisserà i criteri di operatività della piattaforma e l'utente si limiterà alla realizzazione delle applicazioni a lui necessarie dovendo adeguarsi al sistema messo a sua disposizione. Si pensi, ad esempio, all'ipotesi in cui il fornitore opti per un infrastruttura basata su *Linux*, *Apache*, MySQL e PHP; in questo caso il fruitore del servizio deve obbligatoriamente scrivere l'applicazione utilizzando il linguaggio di programmazione PHP ed una base dati MySQL poiché, laddove volesse utilizzare un altro linguaggio o utilizzare un'altra base dati, dovrà optare per un altro fornitore PaaS o, in alternativa, dovrà scegliere un servizio IaaS definendo direttamente la configurazione sistemistica sulla base delle proprie esigenze.

La terza categoria di servizi, infine, è quella nota come *Software as a Service* che identifica applicazioni *software* che funzionano nella nuvola e sono accessibili all'utente tramite *internet* secondo un modello di distribuzione che consente la fruizione del *software* direttamente tramite un *browser* senza la necessità di installare nulla in locale (es. *Gmail*, *Dropbox*, *Facebook*, *etc.*).

L'offerta IaaS, come anticipato, è prevalentemente rivolta ad imprese e ad altri intermediari di *internet* laddove i servizi PaaS possono essere direttamente utilizzati da sviluppatori con adeguate conoscenze tecniche e, quelli SaaS, da utenti dotati anche di minime competenze tecnologiche.

3.- *I modelli di distribuzione dei servizi cloud.*

I modelli di distribuzione del *cloud computing* sono essenzialmente il *public cloud*, il *private cloud*, il *community cloud* e l'*hybrid cloud*[18].

Il *public cloud*[19], noto anche come *external cloud*, è, indubbiamente, la forma di distribuzione più diffusa in cui i servizi erogati dal *cloud provider* sono aperti al pubblico degli utenti che possono accedervi, senza particolari restrizioni, gratuitamente (con o senza registrazione) o a pagamento.

Nel *public cloud* l'infrastruttura è di proprietà di un fornitore che, avendone il pieno controllo, mette a disposizione di utenti, aziende ed enti pubblici il proprio sistema con la condivisione di capacità elaborativa, applicazioni e *storage*.

I benefici scaturenti dall'utilizzo di questo modello sono sicuramente numerosi, basti pensare all'abbattimento dei costi ed alla possibilità di ribaltare la responsabilità connessa alla gestione dell'infrastruttura sul *provider* che assume un ruolo fondamentale nell'adozione delle misure necessarie a garantire la protezione dei dati trasmessi o elaborati con la stessa tecnologia *cloud*.

La complessità dell'infrastruttura e la frequentissima dislocazione dei *server* al di fuori dei confini nazionali, determina incertezza sull'esatta ubicazione dei dati anche a seguito di eventuali spostamenti dettati da ragioni organizzative.

---

[18] Sul punto, *cfr. "the NIST definition of cloud computing"*, reperibile all'indirizzo *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf*.

[19] Il NIST definisce il *public cloud* come *"the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider"*, *cfr. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf*.

Conseguentemente gli utenti che usufruiscono del *cd. public cloud* temono un'eventuale perdita del controllo dei dati scaturente dalla mancata conoscenza del luogo in cui gli stessi vengono memorizzati e dall'impossibilità di definire una propria *policy* di sicurezza dovendo accettare passivamente quella predisposta dal *provider*.

Il *private cloud*[20], noto anche come *internal cloud*, si caratterizza per un infrastruttura interna ad una singola organizzazione o gestita dalla stessa organizzazione o da un terzo. I relativi servizi sono erogati ad utenti interni e non sono sottoscrivibili da esterni.

L'utilizzo del *private cloud*, simile ai tradizionali *data center*, è teso a massimizzare ed ottimizzare le risorse interne ed a garantire maggiore riservatezza e sicurezza dei dati trattati grazie al controllo diretto, da parte dell'utente, delle macchine su cui sono conservati i dati ed eseguiti i processi potendo, conseguentemente, definire le politiche di sicurezza più opportune. Nel *cloud* interno, in altre parole, i dati restano presso l'organizzazione che, pertanto, riesce a mantenere sugli stessi un controllo pieno ed esclusivo. Il *cloud* privato, se da un lato garantisce maggiormente sicurezza e riservatezza dei dati, dall'altro espone gli utenti a costi più elevati dovuti alla necessità di implementare risorse dedicate.

[20] Il NIST definisce il *private cloud* come *"the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises"*, *cfr. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nist specialpublication800-145.pdf*.

Si parla di *community cloud*[21] quando più organizzazioni condividono la stessa infrastruttura privata nonché le relative politiche di gestione e sicurezza. I servizi sono rivolti esclusivamente agli utenti delle organizzazioni aderenti alla *community*.

L'*hybrid cloud* è il frutto della combinazione tra due o più *cloud* (pubblico, privato e *community cloud*) che, in ogni caso, restano entità autonome collegate tra loro da tecnologia *standard* o *proprietaria* che consente la portabilità dei dati o delle applicazioni. Con il modello ibrido si mira ad ottimizzare le risorse fruendo di servizi (IaaS, PaaS, SaaS) erogati da un'infrastruttura distribuita tra i *data center* del *cloud consumer* e quelli del *provider*. Al *cloud* pubblico possono essere affidati servizi e applicazioni che comportano il trattamento di dati non personali o non sensibili mentre per il trattamento di dati particolarmente delicati per i quali è opportuna l'adozione di più efficaci misure di sicurezza, si potrà ricorrere al *private cloud*.

La distinzione tra i diversi modelli distributivi non ha una valenza esclusivamente tecnica e terminologica poiché la scelta di una tipologia piuttosto che di un'altra è in grado di produrre significative conseguenze giuridiche.

Come anticipato, optando per il modello di *pubblic cloud*, l'utente non avrà la possibilità di negoziare le condizioni di utilizzo ed i termini dell'accordo

[21] Il NIST definisce il *community cloud* come *"the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises"*, *cfr. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nist specialpublication800-145.pdf*.

essendo costretto a rinunciare all'utilizzo del servizio o ad accettarlo così come proposto secondo lo schema del "prendere o lasciare"[22]. Maggiore possibilità di negoziazione dell'accordo si riscontra nel *private cloud* anche se è indubbio che, almeno fino ad oggi, il modello più utilizzato è quello di *public cloud* caratterizzato da una maggiore scalabilità e da costi più contenuti e competitivi.

[22] In relazione ai servizi di *public cloud*, anticipando una riflessione che sarà oggetto di approfondimento in prosieguo, è opportuno rilevare come la prassi contrattuale sia caratterizzata da un'estrema rigidità considerando l'impossibilità per l'utente di incidere sui termini dell'accordo. I contratti, inoltre, nella maggior parte dei casi, si caratterizzano per l'estrema genericità della descrizione dell'oggetto del servizio senza che l'utente sia in possesso di informazioni complete sul tipo di tecnologia utilizzata, sulle misure di sicurezza adottate e sulla localizzazione dei *data center*. I *provider* tendono, inoltre, a limitare la loro responsabilità con clausole di dubbia validità.

Capitolo II
Il *cloud computing* nel diritto internazionale

SOMMARIO: 1. Considerazioni introduttive; 2. Il *cloud computing* e la *governance* di internet; 3. Il contratto internazionale e le fonti del diritto; 4. L'individuazione della legge applicabile al contratto; 5. La risoluzione giudiziale delle controversie; 6. Dalle *Alternative Dispute Resolution* alle *Online Dispute Resolution*.

1.- *Considerazioni introduttive.*

Dopo aver delineato le caratteristiche tecniche del *cloud* evidenziandone finalità ed utilità è opportuno valutare le implicazioni giuridiche che scaturiscono dall'utilizzo crescente di questa nuova tecnologia.

Non ci si soffermerà solo sulle problematiche connesse al rapporto tra fruizione dei servizi *cloud*, *privacy* degli utenti e sicurezza dei dati immessi nella nuvola, ma si analizzeranno anche gli aspetti contrattuali sottesi all'utilizzo del *cloud* tentando di delineare la natura della relazione tra *cloud provider* e utenti fruitori dei servizi.

L'approfondimento della suddetta relazione negoziale risulta fondamentale per una corretta qualificazione giuridica del contratto di volta in volta stipulato, per la determinazione della legge applicabile allo stesso e per l'individuazione sia del giudice competente a risolvere eventuali controversie che delle clausole

contrattuali più rilevanti su cui le parti dovranno prestare particolare attenzione[23].

L'inquadramento del rapporto contrattuale *cloud provider*/*cloud user* può diventare complesso in presenza di elementi di estraneità rispetto ad un dato ordinamento. Oltre alle questioni inerenti l'individuazione della legge applicabile, infatti, è necessario gestire il cd. problema della lingua da utilizzare nella redazione del contratto partendo dalla considerazione che i più importanti operatori del settore *cloud* sono statunitensi e, conseguentemente, i contratti predisposti sono quasi sempre redatti in inglese. La corrispondenza dei termini utilizzati nasconde, spesso, una profonda diversità di significato tecnico giuridico dando adito a possibili, evidenti, rischi di confusione sul tipo di contratto da stipulare e sui servizi da sottoscrivere nonché, in sede di esecuzione del contratto, ad eventuali controversie e discrasie.

Deve rilevarsi, infine, che la stipula dei contratti di *cloud computing* prescinde, nella quasi totalità dei casi, dalla fase della trattativa. La conclusione *on line* tramite l'adesione a moduli e formulari predisposti unilateralmente dai *cloud provider*, infatti, riduce il potere contrattuale dell'utente che si limita a dover valutare l'opportunità o meno di aderire alle offerte predisposte dal fornitore.

2.- *Il cloud computing e la governance di Internet.*

Il *cloud computing* è espressione di *internet* presupposto necessario della sua esistenza e del suo funzionamento. L'utilizzo delle nuove tecnologie

[23] Sul punto, *cfr.* E. BELISARIO, *Cloud computing*, eBook n. 17, Altalex, 2011, 11 ss.

difficilmente può essere inquadrato giuridicamente prescindendo dal mezzo di comunicazione *internet*, il solo a rendere davvero determinante l'innovazione tecnologica nei processi produttivi, organizzativi ed amministrativi.

Internet come *medium*, come strumento di comunicazione, infatti, consente di aggirare barriere e distanze, incidendo in maniera notevole su tutti i predetti processi.

Il diritto quale complesso di norme che regolano l'organizzazione di uno Stato, qualunque sia la sua forma, necessita di un "dove"! Il problema del *cyberspazio* è che non c'è un dove poiché il territorio globale di *internet* è virtuale. Le peculiarità della rete, infatti, sono costituite dalla grande difficoltà di collocare geograficamente i soggetti che vi operano e contestualmente dalla particolare attitudine alla diffusione di informazioni ed alla realizzazione di negozi giuridici dialogando, anche in tempo reale, con utenti di tutto il mondo, proprio in virtù della menzionata aspazialità.

L'individuazione della legge applicabile agli atti compiuti via *internet* costituisce, evidentemente, un problema di carattere generale posto che l'individuazione della fonte del diritto applicabile alle attività di rilevanza giuridica svolte sul *world wide web,* è fondamentale per la concreta determinazione del "diritto" applicabile e della giurisdizione relativa.

I singoli diritti nazionali sono ormai sempre più inadeguati a regolare i fenomeni dell'economia globalizzata che, in presenza di un *cyberspazio* caratterizzato come già detto dalla aterritorialità, oltrepassano il classico "limite territoriale" del diritto.

L'assenza di certezza e l'approccio ancora empirico alla problematica segnalata del "quale diritto e quale giudice", incide negativamente sulle opportunità che la rete e l'*Information and Communication Technology* (ICT) in genere, sono in grado di offrire non solo al mondo produttivo ma anche alla stessa organizzazione amministrativa statuale.

Il diritto deve individuare nuove forme di regolamentazione in grado di disciplinare l'economia elettronica internazionale prescindendo da qualsiasi legame materiale con il territorio.

Le soluzioni fino ad ora prospettate nel tentativo di individuare la giusta *governance* di *internet*[24] sono individuabili nell'applicazione del diritto vigente, suddiviso a sua volta in normativa statale o convenzionale, nella necessità di adeguare il diritto e le sue fonti ai nuovi fenomeni giuridici del *cyberspazio*, nell'assenza totale di regole autoritative lasciando all'autoregolazione il compito di creare un ordine equilibrato nonché nella realizzazione di un ordinamento speciale dotato di regole proprie, una *lex informatica*, insomma, in grado di risolvere con soluzioni di carattere tecnologico universalmente condivise, i problemi di coordinamento delle legislazioni nazionali.

La convinzione è che la soluzione debba essere ricercata, come spesso accade, in una giusta via di mezzo ritenendo non soddisfacente tanto la soluzione che lega la *governance* di *internet* all'applicazione del diritto vigente

[24] In argomento, *ex plurimis*, G. FINOCCHIARO, Lex mercatoria *e commercio elettronico. Il diritto applicabile ai contratti conclusi su* Internet, in *Contratto e impr.*, 2001, 571 ss.; ID., *Diritto di internet*, Bologna, 2008; U. DRAETTA, *Internet e commercio elettronico nel diritto internazionale dei privati*, Milano, 2005; C. ROSSELLO, *Commercio elettronico*, Milano, 2006, 8; A. PAPA, *Espressione e diffusione del pensiero di internet*, Torino, 2009; G. DE MINICO, *Internet. Regola e anarchia*, Napoli, 2012.

quanto quella che la lega alla creazione di una regolamentazione speciale di natura tecnologica che avverrebbe al di fuori di qualsiasi processo democratico di decisione.

La *lex informatica*, infatti, rimetterebbe l'adozione delle regole tecniche ai soggetti che, dettandone gli *standard*, regolano il *web* sotto il profilo tecnologico con un grave rischio per i diritti e le libertà degli utenti. I Governi dovrebbero acquisire maggiore consapevolezza del ruolo cardine svolto da tutti i soggetti che, a diverso titolo, gestiscono il *web* regolandone di fatto il funzionamento a scapito di una *governance* democratica e rappresentativa di tutti i soggetti che a vario titolo operano in *internet*. Solo una concreta presa di coscienza ed un deciso intervento nel settore eviterà che *internet* possa perdere il suo più grande pregio: essere strumento di libertà ed uguaglianza sostanziale.

Le possibili fonti di regolamentazione di *internet* – da individuare con riferimento ai modelli centralizzati di produzione delle regole, nel diritto internazionale, nel diritto comunitario e nel *soft law* che, però, a differenza dei primi due, produce modelli normativi, linee guida e raccomandazioni prive di portata precettiva e con riferimento, invece, ai modelli decentralizzati di produzione delle regole e nell'autoregolamentazione – non devono essere considerate autonomamente ed in rapporto di esclusione reciproco ma, piuttosto, quali strumenti concorrenti in grado di interagire e sopperire reciprocamente alle rispettive carenze a vantaggio della disciplina di un fenomeno complesso qual è *internet*.

Il diritto di *internet* non può che essere immaginato come un diritto globale ed elastico caratterizzato dalla partecipazione di un soggetto pubblico alla

produzione spontanea delle regole per tutelare il popolo della rete che diversamente, con un'autoregolamentazione pura, subirebbe il potere "negoziale" e "normativo" dei gruppi forti – spesso detentori della tecnologia o comunque in grado di dettarne gli *standard* – in grado di incidere sulla definizione delle stesse regole formalmente concordate ma di fatto disequilibrate dalla riferita asimmetria di potere.

Il ruolo di legislatore di *internet*, quale soggetto pubblico che indirizzerà l'autoregolamentazione nell'ambito del modello di *co-regulation*, in ragione dell'estensione globale della rete, dovrà essere assunto dalla comunità internazionale interamente intesa o nelle sue articolazioni eventualmente definite[25].

Fin quando non si disporrà di regole uguali e liberali per disciplinare il *web* e, conseguentemente, l'utilizzo di tecnologie come quella *cloud*, sarà necessario guardare al contratto quale strumento necessario per definire le prestazioni oggetto dello stesso e le modalità con cui queste ultime devono essere rese nonché per regolare, in astratto, le questioni potenzialmente idonee a generare un conflitto.

Un contratto ben strutturato e trasparente consente, con specifico riferimento al *cloud computing*, di prevenire situazioni di conflitto; l'utente, infatti, sarà in grado di valutare preventivamente il servizio offerto, la qualità delle prestazioni e le garanzie in merito al trattamento dei dati. Si riuscirà a mantenere un controllo, seppur indiretto, sui propri dati che, nella maggior

[25] Per una completa e approfondita analisi sul diritto giusto per *internet*, *cfr.* l'autorevole lavoro di G. DE MINICO, *cit.*, 5 ss. Sul tema del candidato ideale al ruolo di legislatore di *internet* v. anche M. VIGGIANO, *Internet, Informazione, regole e valori costituzionali*, Napoli, 2010, 57 ss.

parte dei casi, per ragioni insite nello stesso funzionamento del *cloud*, sono allocati in infrastrutture estranee al fruitore di servizi *cloud*.

Considerando che il *cloud* ha una connotazione spiccatamente transnazionale, assumono grande rilievo le questioni relative alla legge applicabile al contratto ed all'individuazione del giudice competente a risolvere gli eventuali conflitti scaturenti dalla sua esecuzione. La certezza normativa è, infatti, determinante per un impiego sempre crescente del *cloud computing*; le divergenze e le differenti tutele apprestate da distinti ordinamenti, infatti, potrebbero essere tali da annullare, in caso di contenzioso, i benefici connessi all'uso della tecnologia *cloud*[26].

3.- *Il contratto internazionale e le fonti del diritto.*

Il contratto relativo all'erogazione di servizi *cloud* deve essere considerato un contratto internazionale ogni qual volta presenta elementi di estraneità rispetto all'ordinamento italiano di riferimento contrapponendosi, così, ai contratti con elementi essenziali tutti rinvenibili all'interno di un unico Paese e, conseguentemente, di un unico ordinamento.

L'accordo tra due o più soggetti appartenenti a diversi Paesi, avendo questi il proprio centro di affari in Stati differenti, spesso anche connotati da tradizioni giuridiche profondamente diverse, deve essere sicuramente considerato internazionale. Tale carattere può essere assunto anche dagli accordi intercorrenti tra soggetti appartenenti ad uno stesso Paese, i cui effetti giuridici, però, non si esauriscono all'interno del proprio Stato, ma si

[26] Sul punto, v. E. BELISARIO, *op. cit.*, 13 ss.

riverberano anche in Paesi stranieri, e che, pertanto, presentano altri tipi di collegamento con l'esterno (si pensi, ad esempio, ad un *cloud provider* italiano che utilizza *server* proprietari o di terzi fornitori localizzati in paesi *extra* europei).

Il coinvolgimento di sistemi giuridici stranieri determina la necessità di un'attenzione maggiore rispetto a quella prestata ai rapporti interni al Paese, scaturente dall'esistenza di "variabili" del tutto nuove rispetto a quelle interne.

La centralità svolta dal contratto e, in particolare, dalla scelta della legge applicabile allo stesso, è il frutto dell'assenza di un sistema coordinato ed organico di norme giuridiche a cui fare riferimento per colmare eventuali lacune e discrasie interpretative, o per fronteggiare le complessità ed atipicità che caratterizzano i rapporti tra parti contrattuali di Paesi differenti; una regolamentazione atta, cioè, ad operare in funzione integrativa delle pattuizioni contenute nell'accordo sottoscritto dalle stesse parti.

Da un valutazione del sistema delle fonti disciplinanti la contrattualistica internazionale emerge l'inadeguatezza dell'attuale quadro giuridico[27] e l'incapacità del diritto a star dietro lo sviluppo dell'economia; la conclusione di negozi transnazionali che in passato costituiva una circostanza eccezionale, coinvolgendo pochi soggetti realmente specializzati nel settore, è diventata oggi anche grazie all'avvento di *internet*, di grandissima attualità con

[27] Sul punto, v. R. DAVID, *Le droit du commerce International,* Paris 1987, p. 11 ss.

conseguente difficoltà di regolamentazione stante l'assenza di un autonomo sistema normativo di riferimento[28].

Se da un lato, dunque, si è tentato di parlare di tramonto del monopolio della normativa nazionale, grazie ad una crescente affermazione ed al rafforzamento del ruolo svolto dalle codificazioni non solo europee, ma più in generale internazionali, dall'altro, però, ci si scontra con la continua necessità di dover far pur sempre riferimento ai singoli sistemi giuridici nazionali, con tutte le criticità che ne conseguono in tema di eccessiva frammentarietà della disciplina applicabile.

In un mercato sempre più globalizzato e universale[29], governato dall'intrecciarsi di una complessità e varietà di fonti giuridiche, si fa sempre più spesso leva sull'autonomia contrattuale[30] riconosciuta dalla maggior parte degli Stati[31]. Detta autonomia regola le questioni più rilevanti dei contratti internazionali e, come anticipato, si manifesta nella determinazione del contenuto del contratto, nella scelta della legge applicabile al negozio e nella scelta della modalità di risoluzione delle possibili controversie, attribuendo allo

---

[28] S. M. CARBONE, R. LUZZATTO, *Il contratto internazionale,* Torino, 1994, p. 1, ove si è evidenziato che manca *"da un punto di vista giuridico una disciplina unitaria, che sia posta in essere da fonti dotate di efficacia normativa estesa all'intera dimensione"*.

[29] V. DE NOVA, *Introduzione,* in *Fonti e tipi del contratto internazionale*, Milano, 1991, p. 2, che parla di *"un traffico di fonti molto affollato"*.

[30] V. GIARDINA, *L'autonomia delle parti nel commercio internazionale*, in *Fonti e tipi del contratto internazionale* (a cura di DRAETTA e VACCA), Milano, 1991, p. 33 ss.

[31] Sull'importanza dell'autonomia contrattuale nel commercio internazionale, v. S. M. CARBONE, *Autonomia privata e contratti internazionali,* in *Nuova giur. civ.,* 1992, II, p. 282 ss.; ID, *Autonomia privata nei rapporti economici internazionali e suoi limiti*, in *Riv. dir. internaz. privato e proc.,* 2007, p. 891 ss.

stesso contratto un ruolo centrale nella gestione dell'affare economico transnazionale[32].

Laddove i contraenti non disciplinano dettagliatamente tutti gli aspetti del loro rapporto il negozio sarà regolato dalla legge nazionale individuata secondo le regole di diritto privato internazionale.

Il diritto comunitario - sforzandosi di dettare una normativa uniforme per l'Unione Europea - è, senza alcun dubbio, fonte di regolazione dei rapporti giuridici all'interno dell'ordinamento europeo laddove, fuoriuscendo dal contesto U.E., le convenzioni internazionali svolgono un ruolo importantissimo nell'ottica dell'applicazione uniforme del diritto commerciale internazionale.

Dette convenzioni, come è noto, si articolano in convenzioni in materia di diritto internazionale privato, convenzioni di diritto processuale internazionale e convenzioni di diritto materiale uniforme.

Le prime sono quelle relative a quella branca dell'ordinamento che mira ad individuare il diritto sostanziale applicabile alle fattispecie che presentano significative connessioni con diversi sistemi giuridici nazionali[33]. Attraverso di esse sarà possibile individuare un criterio di collegamento omogeneo in grado di ricondurre la data fattispecie ad una precisa normativa nazionale, evitando,

---

[32] Su tale impostazione, v. F. BORTOLOTTI, *Drafting and Negotiating International Contract. A practical guide,* Parigi, 2008; S. M. CARBONE, R. LUZZATTO, *Il contratto internazionale*, *cit*; U. DRAETTA, *Il diritto dei contratti internazionali,* vol. I, *La formazione dei contratti*, Padova, 1985; vol. III, *La patologia dei contratti,* Padova, 1988; A. FRIGNANI, *Il diritto del commercio internazionale. Manuale teorico-pratico per la redazione dei contratti,* Milano, 1990; ID., *Il contratto internazionale,* in *Trattato di diritto commerciale e di diritto pubblico dell'economia,* diretto da F. GALGANO, vol. XII, Padova, 1990.

[33] Il diritto internazionale privato, infatti, non è finalizzato alla disciplina materiale del rapporto giuridico, ma all'individuazione della cd. *lex causae* in base alla quale regolare rapporti che presentino elementi di estraneità rispetto all'ordinamento statale nel quale è sorta la controversia.

così, conflitti derivanti dall'eterogeneità dei sistemi di diritto internazionale privato utilizzati dai singoli Stati[34].

Le convenzioni di diritto processuale internazionale[35], a loro volta, mirano ad elaborare criteri uniformi per l'individuazione dell'Autorità giurisdizionale competente e per il riconoscimento delle sentenze straniere, o tendono ad una disciplina uniforme in materia di arbitrato internazionale con l'obiettivo di semplificare le modalità di risoluzione delle controversie commerciali internazionali.

Le convenzioni di diritto materiale uniforme, infine, dettano una disciplina sostanziale ed omogenea rispetto a specifici istituti o contratti; per tale ragione sono in grado di fornire un contributo più ampio al tentativo di superare le divergenze tra le singole normative nazionali. Nel momento in cui la convenzione è sottoscritta e ratificata, infatti, le disposizioni previste dalla stessa andranno ad inserirsi nell'alveo dell'ordinamento nazionale, regolando quella fattispecie in modo uniforme rispetto a quanto previsto dagli altri Stati firmatari.

Non tutte le convenzioni, però, hanno una portata imperativa, dovendo tener presente anche la sussistenza di quelle aventi contenuto meramente dispositivo e come tale derogabile, come ad esempio la Convenzione di Vienna del 1980 in materia di compravendita internazionale di merci, la cui disciplina speciale non sostituisce necessariamente quella interna.

---

[34] *Cfr.*, in via esemplificativa, la Convenzione di Roma del 1980 che ha introdotto nei Paesi che hanno ratificato la stessa un sistema uniforme di diritto internazionale privato in materia di obbligazioni contrattuali.

[35] V., a titolo esemplificativo, la Convenzione di Bruxelles del 1968, di Lugano del 1988 e la Convenzione dell'Aja del 2005.

Le Convenzioni, in ogni caso, nonostante il loro indubbio valore, sono esposte al rischio di una successiva interpretazione difforme, in considerazione del fatto che le stesse saranno, comunque, applicate dai giudici nazionali, alla luce di concetti ed istituti propri del diritto interno[36].

Per superare tale criticità è necessario che i giudici nazionali, all'atto di interpretare le norme uniformi, tengano presenti le sentenze dei giudici stranieri e gli orientamenti consolidatisi in materia[37].

La prassi del commercio internazionale, distanziandosi sempre più dalle singole normative nazionali, tende di frequente ad avvalersi dei *cd.* usi commerciali, la cui applicabilità ed efficacia è comunque soggetta ai limiti ed alle condizioni previste dalla legge applicabile al contratto e dalle convenzioni vigenti di diritto materiale uniforme[38].

Parallelamente allo sforzo posto in essere per un'uniformazione legale o ufficiale della disciplina applicabile ai contratti internazionali attraverso leggi, convenzioni o usi, è opportuno segnalare il tentativo volto ad un'opera di raccolta di tutte le regole uniformi seguite negli affari, che possono essere richiamate dalle parti, per *relationem*, ed inserite nel contratto. Pur restando la loro applicazione subordinata ad una precisa volontà delle parti di richiamarle,

---

[36] *Cfr.* A. FRIGNANI, M. TORSELLO, *Il contratto internazionale, Diritto comparato e prassi commerciali*, Padova, 2010, p. 37.

[37] In termini *cfr*. l'art. 2, co. 2, l. 318/95 in materia di diritto internazionale privato, ai sensi del quale *"nell'interpretazione di tali convenzioni si terrà conto del loro carattere internazionale e dell'esigenza della loro applicazione uniforme"*.

[38] Nell'ordinamento italiano si distinguono, ad esempio, gli usi normativi, disciplinati dall'art. 8 delle Disposizioni preliminari al codice civile, dagli usi negoziali, ex art. 1340 c.c.. I primi presentano un ambito di applicazione piuttosto limitato, in quanto laddove operanti nelle materie già disciplinati da leggi e regolamenti sono applicabili solo se dagli stessi richiamati; i secondi, al contrario, consentono di interpretare le clausole ambigue presenti in un contratto facendo riferimento a ciò che si pratica normalmente nel luogo in cui lo stesso è stato concluso e possono anche derogare alle norme dispositive.

in esplicazione della loro autonomia negoziale, il riferimento costante e ripetuto nel tempo può determinare l'insorgere di veri e propri usi commerciali internazionali, al punto da ritenerli implicitamente richiamati nel contratto, anche in assenza di specifico rinvio[39].

Il tentativo di individuare la legge regolatrice del contratto internazionale in un ordinamento autonomo di fonte extrastatuale passa necessariamente attraverso il ruolo svolto dalla *lex mercatoria* che, come è noto, comprende quel complesso di regole, di natura prevalentemente consuetudinaria o elaborate dalla giurisprudenza arbitrale, volte a disciplinare i contratti internazionali ed i rapporti ad essi sottesi ed a risolvere, attraverso il ricorso a procedure arbitrali, le controversie che possono scaturire dagli stessi contratti[40].

Con la *lex mercatoria*, in altre parole, si mira ad evitare una regolamentazione per il tramite delle disposizioni in materia di diritto internazionale privato o di quelle convenzionali, che potrebbero causare problemi di coordinamento in sede applicativa davanti all'organo giudicante investito della controversia.

Si ritiene, come anticipato, che la *lex mercatoria* non sia uno strumento idoneo a regolamentare il contratto internazionale caratterizzato dalla presenza di *internet* poiché, come già rilavato con riferimento alla cd. *lex* informatica considerata una sorta di seconda *lex* mercatoria, si corre il serio rischio che la

---

[39] Sul punto, v. gli *Incoterms* della Camera di Commercio Internazionale.

[40] V. F. GALGANO, *Lex mercatoria. Storia del diritto commerciale*, Bologna 1993, p. 217 ss.; F. MARRELLA, *La nuova lex mercatoria,* Padova, 2003.; K. P. BERGER, *The Creeping Codification of the New Lex Mercatoria*, Aja, 2010.
Per un raffronto di alcune definizioni, v. M. MUSTILL, *The New Lex Mercatoria: the First Twenty-Five Years,* in *Liber Amicorum Lord Wilberforce*, Oxford, 1987, p. 149 ss. (p. 151). Per un'analisi approfondita v. anche F. DE LY, *International Business Law and "Lex Mercatoria"*, Amsterdam-Londra, 1992, p. 207 ss.

stessa possa restare in balia di una tecnocrazia con spinta autoritativa e pretermissione dei processi decisionali tipici della realtà democratica.

Da ultimo, infine, sempre nell'ottica di giungere ad una produzione di regole extrastatuali per disciplinare i rapporti contrattuali internazionali, si è proceduto all'elaborazione di regole che, convivendo con l'ordinamento nazionale od internazionale, hanno assolto diverse funzioni quali quella di integrare eventuali lacune del contratto, assumere il ruolo di modello di riferimento per il Legislatore fornendo anche i criteri ermeneutici del contratto e della legge applicabile, essere utilizzate come usi normativi o negoziali. Il riferimento è alle raccolte di usi del commercio internazionale a cura dell'UNCITRAL[41] e della Camera di Commercio internazionale, ai principi di diritto europeo dei contratti (cd. PECL) nonché ai principi UNIDROIT[42].

4.- *L'individuazione della legge applicabile al contratto.*

L'individuazione della legge applicabile allo stipulando contratto internazionale è un momento fondamentale per la costruzione di un solido rapporto giuridico poiché, anche se le parti inseriscono all'interno dello stesso contratto una dettagliata regolamentazione del proprio rapporto, non si potrà prescindere da norme imperative inderogabili che dovranno essere applicate al

[41] Commissione delle Nazioni Unite sul diritto del commercio internazionale.
[42] Principi elaborati in seno all'*International Institute for the Unification of Private law* da un gruppo di esperti di diritto del commercio internazionale rappresentanti i diversi sistemi giuridici di *civil law* e di *common law*. L'obiettivo del lavoro è stato quello di elaborare una sorta di codificazione privata tesa a raggruppare la molteplicità di norme ed usi comuni ai differenti Stati, in materia contrattuale, per ottenere regole in linea con i principi ed i criteri applicati nei singoli ordinamenti nazionali garantendo, così, un alto grado di uniformità e di certezza nell'ambito dei rapporti contrattuali internazionali. È importante rilevare che nel preambolo del 1994 degli stessi principi è stato precisato che *"i principi possono applicarsi quando le parti hanno convenuto che il loro contratto sia regolato dai principi generali del diritto, dalla lex mercatoria o simili"*.

contratto e che imporranno determinate scelte ai contraenti. Sul rapporto giuridico in itinere, inoltre, potranno incidere anche le norme dispositive, generalmente derogabili, laddove i contraenti non abbiano disciplinato tutti gli elementi contrattuali. Conseguentemente, per gli aspetti non direttamente regolati, dovrà intervenire la disciplina della legge applicabile al contratto e, pertanto, risulterà fondamentale la conoscenza dell'ordinamento nel quale il negozio giuridico andrà ad innestarsi[43].

Nonostante si affermi sempre più l'importanza di un contratto "*self-regulatory*" o autosufficiente, non è possibile pensare di prescindere totalmente dall'analisi delle norme che saranno applicabili; è opportuno, invece, che l'individuazione della legge sia effettuata ancor prima di procedere alla stipulazione e redazione dello stesso contratto.

Il principale criterio utilizzato per l'individuazione della legge applicabile è quello basato sull'autonoma scelta delle parti che tende a prevalere anche rispetto a quanto eventualmente previsto da convenzioni internazionali o dalle norme di diritto internazionale privato di cui, invece, ci si dovrà avvalere per individuare la legge nazionale di riferimento in mancanza di una precisa ed espressa volontà dei contraenti.

[43] A titolo esemplificativo, si pensi al caso in cui venga inserita nel contratto una clausola penale. Mentre un giurista italiano considererà implicito che, qualora non sia stata espressamente pattuita la risarcibilità del danno ulteriore, il risarcimento è limitato a quanto espressamente pattuito nella clausola *de qua*, l'eventuale sottoposizione del contratto all'applicazione della legge dell'ordinamento tedesco farà sì che potrà sempre essere dimostrato il maggior danno da parte del soggetto in cui favore la penale era stata pattuita.

È opportuno evidenziare che le norme di diritto internazionale privato[44], quali norme interne all'ordinamento giuridico, consentono al giudice, investito di una controversia avente ad oggetto un rapporto internazionale, di individuare, secondo specifici criteri di collegamento, quale sarà la normativa applicabile al caso concreto, non potendo procedere, *sic et simpliciter*, ad un'applicazione della propria normativa interna.

Come anticipato, le norme di diritto internazionale privato prevedono – in virtù di un principio di autonomia in senso internazional privatistico maggiormente rispondente all'esigenza di certezza giuridica[45] – la possibilità, per le parti, di scegliere liberamente la legge che intendono applicare e, solo in assenza di espressa volontà in tal senso, suppliscono a tale lacuna con la determinazione di specifici criteri di collegamento. Questi ultimi, in ogni caso, lasciano comunque un margine di incertezza in merito all'individuazione definitiva della legge applicabile, attesa la discrezionalità del giudice (seppur parziale) al momento di applicazione di tali norme e l'eterogeneità degli specifici sistemi di diritto internazionale privato di ciascun Paese.

Spesso, proprio la riferita eterogeneità, rischia di determinare conseguenze contraddittorie, dal momento che l'applicazione, da parte di giudici di Stati differenti, di norme contenenti diversi criteri di collegamento, può comportare

---

[44] Il diritto internazionale privato può essere definito come *"l'insieme di norme giuridiche le quali, in ogni Stato, identificano la legge applicabile alle fattispecie caratterizzate, appunto, da elementi di estraneità rispetto all'ordinamento statale di cui si tratta, ovvero non totalmente interne ad esso"*, così E. VITTA, F. MOSCONI, *Corso di diritto internazionale privato e processuale,* V ed., Torino 1994, 35.

[45] V. A. SARAVALLE, *Commento all'art. 3*, in *Commentario alla Convenzione di Roma*, in *Nuove leggi civ.*, 1995, p. 942.

l'applicazione, ad una medesima fattispecie, di leggi sostanziali e materiali diverse[46].

Adottando norme private internazionali uniformi, come accaduto nell'ambito dell'Unione Europea con la Convenzione di Roma del 1980 (sostituita, come vedremo di qui a poco, dal Regolamento comunitario 593/2008, cd. Regolamento Roma I), o con Convenzioni in settori particolari, si potrebbe tentare di ridurre tali contraddizioni.

Il problema dell'individuazione della legge applicabile presenta notevoli ulteriori complicazioni nell'ambito dell'arbitrato internazionale a causa della mancanza di un *corpus* di regole da seguire rigidamente[47], a differenza di quanto accade nell'ambito della giurisdizione nazionale grazie alle specifiche previsioni di diritto internazionale privato. Gli arbitri, per superare questa fastidiosa situazione di *impasse*, possono alternativamente scegliere di individuare uno specifico sistema di diritto internazionale privato, grazie al quale accertare, poi, la legge applicabile sulla scorta dei criteri dallo stesso stabiliti, o, in alternativa, di avvalersi di una più ampia discrezionalità individuando direttamente la legge, sulla base di criteri e parametri autonomi, bypassando l'intermediazione delle normative interne (la cd. *voie directe*).

Gli arbitri, quindi, godono di ampia discrezionalità e, conseguentemente, qualora le parti non riescano o non vogliano indicare espressamente la legge

[46] In passato era assai frequente l'ipotesi prospettata, dal momento che il diritto privato internazionale dell'ordinamento italiano prevedeva, quale criterio di collegamento, il luogo di stipulazione del contratto, a differenza della maggior parte degli altri Stati in cui si prediligeva il luogo di esecuzione della prestazione caratteristica. Questa discrasia è stata oggi in parte superata con la ratifica della Convenzione di Roma che ha uniformato i criteri di collegamento almeno nell'ambito U.E.

[47] *Cfr.* A. REDFERN, M. HUNTER, *Law and Practice of International Commercial Arbitration*, Londra, 1991, p. 125-126; H. A. GRIGERA NAON, *Choice-of-law Problems in International Commercial Arbitration*, Tübingen, 1992, p. 83 ss.

che intendono applicare al loro rapporto, e laddove, contestualmente, indichino l'arbitrato come modalità di risoluzione di eventuali controversie, la scelta della normativa operante sarà di fatto rimessa agli stessi arbitri.

Il processo di uniformazione delle regole per la scelta della disciplina applicabile al contratto ha subito, come anticipato, un importante impulso con l'emanazione della Convenzione di Roma del 1980[48], operativa in tutti i Paesi dell'Unione Europea[49], ed oggi sostituita dal Regolamento comunitario 593/2008, *cd.* "Regolamento Roma I", entrato in vigore il 17 dicembre del 2009[50].

---

[48] Ratificata dall'Italia con la l. 18 dicembre 1984, n. 975 ed entrata in vigore il giorno 1 aprile 1991. Sulla portata di tale Convenzione, v. T. BALLARINO, *La Convenzione di Roma sulla legge applicabile alle obbligazioni contrattuali entra in vigore*, in *Banca, borsa ecc.,* 1991, I, p. 649 ss.; A. BONOMI, *Il nuovo diritto internazionale privato dei contratti,* in *Banca, borsa ecc.,* 1992, I, p. 37 ss.; L. F. CARRILLO POZO, *El contrato internacional: la prestación característica,* Bologna, 1994; M. LA ROSA, *Entra in vigore la Convenzione di Roma del 1980 sulla legge applicabile ai contratti,* in *Giur. comm.,* 1991, I, p. 842 ss.; R. LUZZATTO, *L'entrata in vigore della Convenzione di Roma del 1980 e il nuovo diritto internazionale privato dei contratti*, in *Dir. comm. internaz.,* 1991, p. 259 ss.; L. PICCHIO FORLATI, *La Convenzione di Roma del 1980 sulla legge applicabile ai contratti nell'ordinamento italiano*, in E. JAYME, L. PICCHIO FORLATI, *Giurisdizione e legge applicabile ai contratti nella CEE,* Padova, 1990, p. 109 ss.; F. POCAR, *L'entrata in vigore della Convenzione di Roma del 1980 sulla legge applicabile ai contratti,* in *Riv. dir. internaz. privato e proc.,* 1991, p. 249 ss.

[49] L'ordinamento tedesco, però, piuttosto che ritenere applicabili tali disposizioni in via diretta, ha preferito provvedere all'inserimento nel EGBGB di specifiche norme dal contenuto sostanzialmente analogo a quelle della Convenzione in esame.

[50] Quanto alle obbligazioni extracontrattuali, giova menzionare la disciplina dettata dal Regolamento Comunitario 864/2007 (cd. Roma II), entrato in vigore l'11 gennaio 2009. Tale normativa detta una serie di criteri per determinare la legge applicabile alle obbligazioni non derivanti da contratto in materia civile e commerciale (ad es. casi di responsabilità da prodotto, di responsabilità precontrattuale, *etc.*), ogniqualvolta si verifichi un conflitto tra leggi di paesi diversi. Sono espressamente escluse dal campo d'applicazione le obbligazioni extracontrattuali nelle materie fiscali, doganali o amministrative, nonché la responsabilità dello Stato per atti o omissioni nell'esercizio di pubblici poteri (*acta iure imperii*). Anche alcune obbligazioni extracontrattuali rientranti nella materia civile e commerciale, ed espressamente indicate nell'atto, sono escluse dal suo campo di applicazione. In linea di principio, in base ai criteri previsti dal Regolamento, la legge applicabile sarà:
a) quella del paese in cui si verifica il danno; o, in mancanza, b) quella del paese in cui risiedono abitualmente sia il presunto responsabile, sia la parte lesa nel momento in cui il danno si verifica; o, in mancanza, c) quella del paese con cui il fatto illecito presenta collegamenti manifestamente più stretti rispetto ai paesi di cui sopra.

La predetta Convenzione ha carattere universale trovando applicazione anche laddove la legislazione individuata in base ai criteri dalla stessa stabiliti non appartenga ad uno Stato contraente.

Sono esclusi dal suo ambito di applicazione, invece, tutti i contratti che non presentano elementi di estraneità rispetto a un determinato ordinamento giuridico (cd. contratti interni) ed una serie di materie tassativamente indicate dalla stessa Convenzione[51].

Deve rilevarsi, invero, che la Convenzione di Roma, in considerazione di quanto previsto dalla l. 218/95[52], può essere ritenuta idonea, almeno nell'ordinamento italiano, a disciplinare anche le fattispecie normalmente escluse dal suo ambito di applicazione[53].

L'art. 3 della Convenzione, in attuazione del principio più volte menzionato del riconoscimento della massima autonomia negoziale ai contraenti, consente alle parti la libertà di individuare la legge da applicare al contratto[54], indipendentemente dalla sussistenza di un diretto collegamento tra il negozio stipulato ed il Paese prescelto[55].

---

[51] Sono escluse dall'ambito di operatività della Convenzione le obbligazioni derivanti da cambiali, assegni, i *trust*, i contratti di assicurazione per la copertura di rischi localizzati nel territorio delle Comunità Europee, le clausole compromissorie e di scelta del foro, *etc.*

[52] *Cfr.* l'art. 57, l. 218/95 secondo cui le obbligazioni contrattuali sono "in ogni caso" regolate dalla Convenzione di Roma. L'effetto del predetto rinvio è, invero, ridotto dalla previsione secondo cui lo stesso non opera – con conseguente disapplicazione della Convenzione – quando le materie oggetto di esclusione sono disciplinate da altre disposizioni della stessa l. 218/95, da leggi speciali, o da Convenzioni internazionali ratificate dall'Italia.

[53] V. T. TREVES, *Art. 57*, in *Riv. dir. internaz. privato e proc.*, 1995, p. 1178; M. V. BENEDETTELLI, *La legge regolatrice delle obbligazioni contrattuali tra convenzione di Roma e diritto internazionale privato comune*, in *Dir. comm. internaz.,* 1996, p. 715 ss.

[54] *Cfr.* M. GIULIANO, *La loi d'autonomie: le principe et sa justification théorique*, in *Riv. dir. internaz. privato e proc.,* 1979, p. 217 ss.

[55] Nonostante l'ampio margine di scelta riconosciuto ai contraenti, si discute se agli stessi sia consentito anche prescindere totalmente da uno specifico ordinamento statuale ed optare per un sistema a-nazionale, quale quello della *lex mercatoria* o dei Principi *Unidroit.* La risposta a tale interrogativo è fortemente ancorata all'interpretazione che si voglia attribuire alla nozione di

L'opzione deve essere *"espressa, o risultare in modo ragionevolmente certo dalle disposizioni del contratto o dalle circostanze"*, essendo così circoscritta la possibilità di una scelta tacita e negata quella di considerare la *lex fori* una presunzione di automatica volontà delle parti di applicare la normativa dell'ordinamento di appartenenza del giudice designato[56]. Per considerare la *lex fori* elemento riconducibile ad una tacita volontà, è necessario dimostrare che le parti abbiano preso in considerazione il problema della scelta della legge applicabile e che, conseguentemente, la determinazione del giudice competente sia stata effettuata proprio per consentire allo stesso di applicare la normativa del proprio Stato di appartenenza.

L'indicazione della legge applicabile al contratto, se non effettuata espressamente, deve poter essere desunta in maniera certa dal coordinamento tra varie risultanze contrattuali al fine di evitare che un'eccessiva valorizzazione di una volontà tacita o poco chiara delle parti, possa comportare un'ingiustificata compressione del principio di certezza e di ragionevole prevedibilità della legge applicabile al rapporto.

Nel contratto internazionale le parti hanno la possibilità di rimandare, ad un momento successivo, l'individuazione della legge applicabile anche sostituendo quella precedentemente individuata senza che da tale facoltà

"legge applicabile", *ex* art. 3 della Convenzione, che, qualora letta in senso estensivo, sarebbe idonea a ricomprendere anche le fonti in esame. Resta inoltre da sottolineare che siffatto dubbio concerne esclusivamente le ipotesi in cui la controversia venga portata alla cognizione delle giurisdizioni ordinarie, mostrandosi al contrario gli arbitri molto più propensi e disponibili a rispettare una scelta delle parti in tale direzione.

[56] In realtà permane, nell'attuale testo, un unico riferimento in tal senso, prevedendosi che l'accordo delle parti volto all'attribuzione della competenza esclusiva a conoscere eventuali controversie concernenti il contratto ad un determinato giudice nazionale, possa rappresentare un elemento da tenere in considerazione, in aggiunta ad altri, per valutare una scelta tacita dei contraenti in favore di una determinata legge nazionale.

possano scaturire pregiudizi per diritti acquisiti, nelle more, dai terzi[57]. A differenza di ciò che accadeva in passato, è oggi possibile utilizzare, per l'individuazione della legge applicabile, anche la tecnica del *cd. depeçage*, consistente nella possibilità di assoggettare il contratto stipulato a diverse normative. Tale strumento consente di utilizzare le soluzioni più adatte alle esigenze del caso concreto, potendo eventualmente superare il contenuto di norme imperative altrimenti applicabile, mediante il rinvio ad una diversa legge nazionale che disciplini quell'aspetto.

Le parti, in ogni caso, non potranno individuare la legge applicabile al contratto, paralizzando l'operatività delle norme imperative eventualmente in contrasto con le clausole contrattuali.

Laddove non sia stata volontariamente individuata la legge applicabile al contratto, deve rilevarsi che il Regolamento – innovando il modello originariamente previsto dalla Convezione di Roma[58] – ha subordinato l'applicazione del criterio del collegamento più stretto tra il contratto ed il Paese di riferimento all'inutilizzabilità dei criteri specifici dettati per i contratti di vendita, di *franchising*, di distribuzione, *etc.*, e di quello *"del luogo di residenza del soggetto che deve eseguire la prestazione caratteristica"*.

---

[57] Si consideri, ad esempio, la possibilità, per gli arbitri, in un arbitrato internazionale, in assenza di una legge preventivamente precedenza individuata, di sollecitare i contraenti ad accordarsi in quella sede sulla normativa applicabile per una maggiore celerità e snellezza della procedura in essere.

[58] La Convenzione, nella sua previgente formulazione, prevedeva, all'art. 4, come principio cardine per l'individuazione della normativa applicabile al caso concreto, la scelta della legge del Paese con il quale il contratto presentava il collegamento più stretto. La disposizione era poi integrata da una serie di presunzioni che miravano a raggiungere soluzioni uniformi attraverso l'utilizzazione di criteri univoci per i singoli contratti. Nei contratti articolati si riscontravano difficoltà connesse alla non facile individuazione della prestazione principale da eseguire.

Il Regolamento Roma I, inoltre, ha attribuito maggiore importanza, rispetto alla precedente formulazione, al luogo in cui le parti, o i loro intermediari, si trovano al momento di stipulazione del contratto. In presenza della stipula di un negozio tra assenti concluso con una controparte straniera che, però, all'atto della formalizzazione, si trovi nello stesso Stato dell'altra, infatti, dovranno essere rispettati i requisiti formali della legge vigente nel Paese di conclusione dell'affare.

La libertà di scelta della legge applicabile al contratto comporta il rischio che, dall'esercizio dell'autonomia contrattuale, possa scaturire la volontà delle parti di escludere volutamente l'operatività di norme imperative dell'ordinamento che diversamente, in assenza di scelta, avrebbero trovato applicazione.

Invero le parti, pur nel rispetto della libertà di scelta della legge applicabile, sono obbligate all'osservanza di singole norme. Per definire concretamente i contorni della questione prospettata è importante soffermarsi sulla distinzione tra norme "semplicemente imperative" - ovvero inderogabili nel contesto nazionale di riferimento, ma disapplicabili a livello internazionale[59] - e norme "internazionalmente o assolutamente imperative", quali quelle di applicazione necessaria che non sono in alcun modo derogabili. Si tratta, in particolare, di principi e di regole considerate fondamentali dall'ordinamento di riferimento

[59] È opportuno sottolineare che la stessa Convenzione di Roma prevede alcune ipotesi specifiche in cui norme aventi carattere imperativo a livello interno devono essere necessariamente applicate e rispettate a livello internazionale, nonostante il contratto venga di per sé assoggettato ad un'altra normativa. Si consideri, ad esempio, il caso dei contratti con i consumatori, per i quali, al ricorrere di determinate condizioni, è comunque prevista l'operatività delle norme imperative (protettive) del proprio Paese di residenza abituale.

che, a prescindere dalla scelta della legge da applicare al rapporto giuridico, ne impone la necessaria osservanza.

Come è noto, le norme ad applicazione necessaria possono essere ricondotte a due grandi macroaree così individuate: a) norme di applicazione necessaria, applicabili anche a fattispecie non caratterizzate da elementi di estraneità[60], che escludono l'operatività delle norme di conflitto; b) norme espressione di principi di ordine pubblico internazionale che impediscono, conseguentemente, l'attuazione di disposizioni normative individuate in contrasto con gli stessi principi di ordine pubblico internazionale[61].

Il Regolamento Roma I ha parzialmente modificato la stessa nozione di norma di applicazione necessaria, richiedendo che il rispetto delle stesse, a prescindere dalla legge applicabile al contratto, sia ritenuto essenziale dallo Stato per la salvaguardia dei suoi interessi pubblici, quali la sua organizzazione politica, sociale ed economica[62].

Come anticipato, nel momento in cui le parti individuano una determinata legge da applicare al contratto non può escludersi la possibile presenza nell'ordinamento della controparte di norme inderogabili e di ineludibile applicazione; ciò accade soprattutto con riferimento alle disposizioni poste a tutela di contraenti deboli o, più in generale, a tutela di interessi pubblici.

Pertanto, ove non fosse possibile escludere l'operatività di tali norme ad applicazione necessaria, può risultare utile la loro diretta applicazione provando ad individuare, se possibile, soluzioni di compromesso.

---

[60] V. E. VITTA, F. MOSCONI, *Diritto internazionale privato cit*., p. 56.
[61] V. F. BORTOLOTTI, *Manuale di diritto commerciale internazionale*, Padova, I, 2009, p. 315.
[62] Sul punto, *cfr.* art. 9, Regolamento Roma I.

La possibilità di limitare od escludere l'applicazione di tali norme può variare a seconda dell'autorità giurisdizionale chiamata a pronunciarsi sull'eventuale controversia. Il giudice del Paese della controparte senza dubbio andrà ad applicare le norme di ordine pubblico internazionale, disapplicando la legge "estranea" se confliggente; lo stesso potrebbe non accadere laddove la legge applicabile al contratto coincide con quella del Paese a cui appartiene il giudice chiamato ad applicarla che, pertanto, non necessariamente utilizzerà la legge straniera in sostituzione di quella propria.

Un simile approccio può determinare il mancato riconoscimento della sentenza non rispettosa delle norme di applicazione necessaria e contraria all'ordine pubblico internazionale.

Laddove una delle parti contrattuali è un consumatore (*cd.* contratto B2C), cosa molto frequente nell'ambito dei contratti di *cloud computer*, soprattutto con riferimento ai servizi SaaS, all'atto negoziale sarà applicabile, ai sensi del Regolamento Roma I, la legge del Paese in cui risiede il consumatore purché il professionista svolga o diriga la propria attività verso tale luogo.

Nel caso del *cloud computing* ciò accade con evidenza se si considera che gli utenti, dislocati in varie parti del globo, sono raggiunti dagli specifici servizi *cloud* tramite *internet* che funge anche da pervasiva forma di comunicazione pubblicitaria. Conseguentemente, quindi, non potranno essere eluse le norme imperative del Paese di residenza del consumatore ogni qual volta il sito del *provider* è visibile nel relativo territorio.

Anche il consumatore può optare per la previsione che consente la libertà di scelta della legge applicabile ma, a sua tutela, l'eventuale scelta potrà essere

indirizzata ad un ordinamento che garantisce un livello di garanzia pari o superiore a quella assicurata dalla normativa nazionale di riferimento.

È opportuno rilevare, con specifico riferimento all'ordinamento italiano, che il Codice del Consumo[63] ha esplicitamente escluso la possibilità che, in presenza di un fornitore straniero, il consumatore possa essere privato della tutela minima apprestata attraverso l'inserimento, in contratti standardizzati, di clausole che prevedono l'applicazione di una normativa straniera[64].

Dalla possibilità di applicare il Codice del Consumo ai contratti *cloud*, scaturisce un'altra importante conseguenza rappresentata dall'utilizzabilità dell'azione collettiva di cui all'art. 140 *bis*, d.lgs. 206/05 ogni qual volta se ne presenti la necessità[65].

Al tema della legge applicabile al contratto è strettamente connesso quello dell'individuazione del foro competente. Tale ultima scelta è spesso effettuata per controbilanciare quella relativa alla normativa applicabile o, come anticipato, per far fronte all'ipotesi in cui la legge non sia stata individuata dai contraenti con la conseguente operatività del meccanismo della *lex fori*[66].

La possibilità riconosciuta alle parti di determinare non solo la legge applicabile, ma anche il foro competente, aumenta il rischio che si possa

---

[63] D.lgs. 06 settembre 2005, n. 206, Codice del Consumo.

[64] L'art. 143, d.lgs. 206/05 statuisce che *"i diritti attribuiti al consumatore dal codice sono irrinunciabili. È nulla ogni pattuizione in contrasto con le disposizioni del codice.*
Ove le parti abbiano scelto di applicare al contratto una legislazione diversa da quella italiana, al consumatore devono comunque essere riconosciute le condizioni minime di tutela previste dal codice".

[65] A titolo esemplificativo si consideri l'ipotesi di temporanea inaccessibilità alle risorse del *cloud* o a fortuite rilevazioni a terzi di dati o in informazioni dell'utente; in tali circostanze gli utenti danneggiati potrebbero avvalersi del rimedio della *class action*.

[66] Come anticipato, non è corretta la convinzione secondo cui l'individuazione del foro competente comporta automaticamente l'applicazione del diritto di quel determinato Paese, sul punto *cfr.* il successivo § 5.

generare il fenomeno del *forum shopping*, caratterizzato dal tentativo, della parte che vuole intentare un'azione giudiziaria, di scegliere la giurisdizione considerata più favorevole e dalla quale si prevede di ottenere, comunque, spese processuali più contenute e sostenibili.

Sarà necessario, infine, verificare l'efficacia della sentenza nello Stato dell'altro contraente poiché i provvedimenti giudiziari sono direttamente riconosciuti solo in presenza della sottoscrizione di trattati di reciproco riconoscimento laddove, nel caso della loro assenza, la pronuncia potrebbe anche non essere considerata valida.

5.- *La risoluzione giudiziale delle controversie.*

Dopo aver affrontato il tema dell'individuazione della legge applicabile al contratto internazionale, è necessario soffermarsi sulle questioni relative alla scelta del giudice deputato a risolvere le controversie che dovessero scaturire dalla attuazione dello stesso. La tendenza è quella di prevedere specifiche clausole tese a devolvere potenziali futuri contenziosi a giudici individuati anticipatamente o ad arbitri, sulla scorta di una valutazione preventiva dell'efficienza di un'eventuale risposta giudiziaria atteso che la stessa - se inefficace per tempi, costi e garanzie - renderà opportuna l'introduzione di clausole contrattuali idonee ad evitare il sorgere della controversia ed il conseguente ricorso all'Autorità giudiziaria[67].

[67] Si consideri, ad esempio, la possibilità, in un contratto di compravendita, di richiedere il pagamento anticipato o la garanzia di un terzo laddove, a seguito di un'approfondita valutazione, ci si dovesse rendere conto che, in caso di inadempimento, il ricorso all'Autorità giudiziaria difficilmente consentirebbe di raggiungere il risultato previsto contrattualmente.

La scelta del giudice competente a risolvere possibili controversie, come anticipato, non comporta l'automatica operatività della sua legge nazionale posto che lo stesso potrà essere chiamato ad applicare la normativa di un Paese diverso, individuata come legge regolatrice del contratto.

Per inquadrare le principali questioni legate alla scelta del giudice devono essere considerate le determinazioni dei singoli Stati attesa l'inesistenza di un sistema uniforme a livello internazionale. I diversi Paesi, infatti, definiscono autonomamente, tanto i limiti della competenza internazionale dei propri giudici, quanto il valore da attribuire ai provvedimenti emessi da Autorità giudiziarie straniere[68] con le sole eccezioni previste dalla Convenzione Europea di Bruxelles (sostituita prima dal Regolamento 44/2001 e poi dal Regolamento 1215/12[69]) e da quella di Lugano del 2007, recanti criteri uniformi di giurisdizione per i Paesi aderenti.

L'assenza di una disciplina uniforme e, soprattutto, il mancato coordinamento tra le diverse normative nazionali, può determinare un evidente rischio di litispendenza di una controversia innanzi a giudici appartenenti a Stati differenti con probabili, conseguenti, provvedimenti contrastanti.

[68] In Italia si è passati da un sistema autarchico delineato dal codice di procedura civile del 1942 ad un sistema più flessibile e propenso al riconoscimento dei provvedimenti stranieri a seguito dell'entrata in vigore della l. 218/95.

[69] Il Regolamento CE 44/2001 sulla competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, ha sostituito, a far data dal 01.03.12, la Convenzione di Bruxelles nei rapporti tra gli Stati membri della Comunità Europea, salva l'esclusione di determinati territori, prevista dall'art. 68 dello stesso Regolamento in combinato disposto con l'art. 299 del Trattato istitutivo della Comunità Europea, ai quali continuerà ad applicarsi la Convenzione di Bruxelles. Il nuovo Regolamento UE 1215/2102 ha sostituito, a far data dal 10 gennaio 2015, il Regolamento 44/01 e costituisce, oggi, lo strumento normativo volto a disciplinare nell'UE la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale.

Un'eventuale controversia in merito ad un contratto internazionale tra una parte italiana ed una controparte straniera, comporterà la necessità, al fine della individuazione della normativa applicabile, di verificare il domicilio della controparte presupposto, quest'ultimo, per l'applicazione del Regolamento 1215/2012 e della Convenzione di Lugano[70].

In presenza di un domicilio in Paesi extraeuropei o non appartenenti all'*European Free Trade Association*[71], troverà applicazione, in assenza di specifiche Convenzioni bilaterali, la l. 218/95.

Come anticipato, presupposto per l'applicazione del Regolamento 1215/2012 - limitatamente alla materia civile e commerciale, con esclusione di quella fiscale, doganale, amministrativa e delle questioni riguardanti la responsabilità dello Stato per atti od omissioni nell'esercizio di pubblici poteri, lo stato e la capacità delle persone fisiche, le successioni, la sicurezza sociale, i concordati, i fallimenti, il regime patrimoniale dei coniugi e l'arbitrato - è il domicilio del convenuto in uno Stato contraente[72].

---

[70] La Convenzione di Lugano del 16 settembre del 1988 prevede un regime sostanzialmente equivalente a quello della Convenzione di Bruxelles (e dunque a quello dell'attuale Regolamento) limitato oggi ai rapporti con Islanda, Norvegia e Svizzera, a seguito dell'adesione all'U.E. di Austria, Finlandia e Svezia (che con i precedenti tre formavano l'EFTA, ovvero l'Associazione Europea di Libero Scambio). La differenza fondamentale tra le due Convenzioni è rinvenibile nel fatto che la Convenzione di Bruxelles, a differenza di quella di Lugano, ha attribuito alla Corte di Giustizia Europea il potere di risolvere in via pregiudiziale eventuali questioni interpretative sorte in relazione all'applicazione della stessa.

[71] L'Associazione europea di libero scambio (EFTA) è nata nel 1960 su iniziativa dei paesi non aderenti all'allora Comunità economica europea (EEC). Attualmente l'EFTA, a seguito del passaggio dei Paesi aderenti prima alla Comunità economica europea e poi all'Unione Europea, è formata da Islanda, Liechtenstein, Norvegia e Svizzera.

[72] In presenza di un convenuto persona giuridica si farà riferimento alla sede della stessa. È opportuno segnalare che il Regolamento avrà applicazione anche in presenza di convenuti domiciliati in Paesi terzi quando: a) è attribuita una competenza esclusiva all'Autorità giudiziaria di uno Stato contraente; b) le parti, di cui almeno una domiciliata in uno Stato contraente, hanno individuato la competenza di un giudice di uno Stato aderente al Regolamento; c) il convenuto di un Paese terzo ha accettato la competenza, comparendo in giudizio.

Il giudice competente sarà quello del luogo in cui è domiciliato il convenuto laddove non siano applicabili specifiche deroghe in grado di determinare fori esclusivi[73], alternativi o facoltativi rispetto a quello del convenuto.

L'art. 7, n. 1, lett. a) del Regolamento, inoltre, prevede la facoltà, in materia contrattuale, di citare il convenuto, domiciliato nel territorio di uno Stato contraente, *"davanti all'autorità giurisdizionale del luogo di esecuzione dell'obbligazione dedotta in giudizio"*[74], convenendo, così, la parte straniera innanzi al "proprio" giudice.

---

[73] Sul punto, v. art. 24 del Regolamento, secondo cui: *"indipendentemente dal domicilio delle parti, hanno competenza esclusiva le seguenti autorità giurisdizionali di uno Stato membro:*
1) in materia di diritti reali immobiliari e di contratti di locazione di immobili, le autorità giurisdizionali dello Stato membro in cui l'immobile è situato.
Tuttavia, in materia di contratti di locazione di immobili a uso privato temporaneo stipulati per un periodo massimo di sei mesi consecutivi, hanno competenza anche le autorità giurisdizionali dello Stato membro in cui il convenuto è domiciliato, purché il conduttore sia una persona fisica e il locatore e il conduttore siano domiciliati nel medesimo Stato membro;
2) in materia di validità della costituzione, nullità o scioglimento delle società o persone giuridiche, o riguardo alla validità delle decisioni dei rispettivi organi, le autorità giurisdizionali dello Stato membro in cui la società o persona giuridica ha sede. Al fine di determinare tale sede l'autorità giurisdizionale applica le proprie norme di diritto internazionale privato;
3) in materia di validità delle trascrizioni e iscrizioni nei pubblici registri, le autorità giurisdizionali dello Stato membro nel cui territorio i registri sono tenuti;
4) in materia di registrazione o di validità di brevetti, marchi, disegni e modelli e di altri diritti analoghi per i quali è prescritto il deposito ovvero la registrazione, a prescindere dal fatto che la questione sia sollevata mediante azione o eccezione le autorità giurisdizionali dello Stato membro nel cui territorio il deposito o la registrazione sono stati richiesti, sono stati effettuati o sono da considerarsi effettuati a norma di un atto normativo dell'Unione o di una convenzione internazionale.
Fatta salva la competenza dell'Ufficio europeo dei brevetti in base alla convenzione sul rilascio di brevetti europei, sottoscritta a Monaco di Baviera il 5 ottobre 1973, le autorità giurisdizionali di ciascuno Stato membro hanno competenza esclusiva in materia di registrazione o di validità di un brevetto europeo rilasciato per tale Stato membro;
5) in materia di esecuzione delle decisioni, le autorità giurisdizionali dello Stato membro nel cui territorio ha o ha avuto luogo l'esecuzione".

[74] Il luogo di esecuzione dell'obbligazione dedotta in giudizio è stato individuato, con riferimenti ai contratti di compravendita dei beni, nel *"luogo, situato in uno Stato membro, in cui i beni sono stati o avrebbero dovuto essere consegnati in base al contratto"* (*cfr.* art. 7.1, lett. b). A tal proposito la Corte di Giustizia CE, con la sentenza del 25 febbraio 2010 (*Car Trim GmbH c. Key Safety System Srl*, causa C-381/08 CE), ha ritenuto che, ogniqualvolta non sia possibile determinare il luogo di consegna in base alle pattuizioni contrattuali (e quindi nel contratto non sia indicato in maniera sufficientemente chiara il luogo di consegna dei beni venduti), tale luogo dovrà intendersi essere quello della consegna materiale dei beni

La predetta deroga trova applicazione solo per le obbligazioni contrattuali e, conseguentemente, quelle non rientranti in tale fattispecie, se configurabili come obbligazioni extracontrattuali, potranno essere soggette alla deroga di cui dall'art. 7, n. 2 che, in materia di illeciti civili dolosi o colposi, stabilisce la possibilità di citare il convenuto domiciliato in uno Stato contraente *"davanti al giudice del luogo in cui l'evento dannoso è avvenuto o può avvenire"*.

In presenza di una pluralità di convenuti, ai sensi dell'art. 8, n. 1 del Regolamento, chi è domiciliato nel territorio di uno Stato contraente può essere citato a comparire davanti al giudice del luogo in cui uno qualsiasi degli altri convenuti è domiciliato, *"sempre che tra le domande esista un nesso così stretto da rendere opportuna una trattazione unica ed una decisione unica onde evitare il rischio di giungere a decisioni incompatibili derivanti da una trattazione separata"*.

La Corte di Giustizia – pur non pronunciandosi direttamente sull'art. 8, n. 1 del Regolamento ma, piuttosto, sulla stessa disposizione contenuta nella Convenzione di Bruxelles – ha avuto modo di precisare che la disposizione *de qua* può trovare applicazione anche quando le azioni, esperite nei confronti dei diversi convenuti, sono fondate su differenti presupposti normativi[75] purché, tra le stesse, ci sia uno stretto vincolo di connessione *"tale da rendere opportune*

---

all'acquirente, ossia il luogo in cui l'acquirente acquisisce la disponibilità materiale di detti beni.
Con riferimento, invece, ai contratti aventi ad oggetto la prestazione di servizi, il luogo di esecuzione dell'obbligazione dedotta in giudizio è stato individuato nel *"luogo, situato in uno Stato membro, in cui i servizi sono stati o avrebbero dovuto essere prestati in base al contratto"* (*cfr.* art. 7.1, lett. b).

[75] Si consideri, ad esempio, la proposizione congiunta di una domanda contrattuale e di una extracontrattuale.

una trattazione e decisione uniche per evitare soluzioni che potrebbero essere tra di loro incompatibili se le cause fossero decise separatamente"[76].

Scatterà una deroga al foro generale del convenuto anche nell'ipotesi di chiamate in garanzia o di altra chiamata di terzo; un soggetto domiciliato in uno Stato contraente, diverso da quello del giudice adito in via principale, infatti, potrà essere citato *"davanti all'autorità giurisdizionale presso la quale è stata proposta la domanda principale, a meno che quest'ultima non sia stata proposta solo per distogliere colui che è stato chiamato dalla sua autorità giurisdizionale naturale"*.

Ai sensi del Regolamento 1215/2012, inoltre, le parti hanno la possibilità di derogare al foro competente determinato sulla scorta delle citate disposizioni. I contraenti, infatti, possono stabilire preventivamente ed in completa autonomia a quale giudice devolvere la conoscenza di una possibile controversia[77] anche

---

[76] V. Corte di Giustizia 11 ottobre 2007, causa C-98/06 *Freeport plc* c. *Olle Arnoldsson,* in *Riv. dir. internaz. privato e proc.* 2008, p. 258 ss.

[77] V. art. 25 del Regolamento in esame, secondo cui *"1. Qualora le parti, indipendentemente dal loro domicilio, abbiano convenuto la competenza di un'autorità o di autorità giurisdizionali di uno Stato membro a conoscere delle controversie, presenti o future, nate da un determinato rapporto giuridico, la competenza spetta a questa autorità giurisdizionale o alle autorità giurisdizionali di questo Stato membro, salvo che l'accordo sia nullo dal punto di vista della validità sostanziale secondo la legge di tale Stato membro. Detta competenza è esclusiva salvo diverso accordo tra le parti. L'accordo attributivo di competenza deve essere:*
a) concluso per iscritto o provato per iscritto;
b) in una forma ammessa dalle pratiche che le parti hanno stabilito tra di loro; o
c) nel commercio internazionale, in una forma ammessa da un uso che le parti conoscevano o avrebbero dovuto conoscere e che, in tale ambito, è ampiamente conosciuto e regolarmente rispettato dalle parti di contratti dello stesso tipo nel settore commerciale considerato.
2. La forma scritta comprende qualsiasi comunicazione con mezzi elettronici che permetta una registrazione durevole dell'accordo attributivo di competenza.
3. L'autorità o le autorità giurisdizionali di uno Stato membro alle quali l'atto costitutivo di un trust ha attribuito competenza a giudicare hanno competenza esclusiva per le azioni contro un fondatore, un trustee o un beneficiario di un trust, ove si tratti di relazioni tra tali persone o di loro diritti od obblighi nell'ambito del trust.
4. Gli accordi attributivi di competenza e le clausole simili di atti costitutivi di trust non sono valide se in contrasto con le disposizioni degli articoli 15, 19 o 23 o se derogano alle norme sulla competenza esclusiva attribuita alle autorità giurisdizionali ai sensi dell'articolo 24.

sottraendosi alla giurisdizione esclusiva dell'autorità giudiziaria dei Paesi membri. Le parti possono indicare più fori alternativi ricomprendendo anche quelli di Paesi in cui non hanno fissato il proprio domicilio.

La scelta del giudice competente, ai sensi del Regolamento 1215/2012, deve essere effettuata rispettando particolari requisiti di forma a garanzia, per i contraenti, della piena conoscenza delle scelte operate.

La clausola deve essere conclusa o provata per iscritto e, a tal fine, è sufficiente la sottoscrizione del contratto recante la deroga[78]. Per la validità della clausola, in altre parole, la forma scritta non è richiesta *ad substantiam*; sarà necessaria, piuttosto, per provare l'esistenza della stessa clausola (forma scritta *ad probationem*). Il requisito è rispettato se la clausola è contenuta in condizioni generali di contratto, predisposte da un solo contraente e riportate sulla parte posteriore del documento, purché le stesse siano espressamente richiamate dal testo sottoscritto.

In presenza di condizioni generali prive di sottoscrizione, invece, la clausola di deroga della competenza soddisferà il requisito della forma scritta *ad probationem*, se l'accordo sottoscritto contiene un esplicito riferimento alle stesse condizioni generali.

Nel caso di un accordo contrattuale raggiunto attraverso lo scambio telematico dei documenti, è possibile che solo una delle parti accetti per iscritto

---

5. Una clausola attributiva di competenza che fa parte di un contratto si considera indipendente dalle altre clausole contrattuali.
La validità della clausola attributiva di competenza non può essere contestata per il solo motivo che il contratto è invalido".

[78] È necessario segnalare che ai sensi dell'art. 25, n. 2, Regolamento 1215/12, in tutti i casi di comunicazione con mezzi elettronici, il requisito della forma scritta si deve ritenere soddisfatto se è possibile una *"registrazione durevole della clausola attributiva di competenza"*.

la clausola inviatale dall'altra parte che, pertanto, non l'ha contestualmente sottoscritta. Il tal caso è pacifico che il requisito della forma scritta, anche solo *ad probationem*, può ritenersi sussistente poiché chi chiede di sottoscrivere la clausola derogatoria della competenza non può, poi, non avere piena consapevolezza della stessa.

In definitiva è possibile rilevare che l'accettazione della clausola derogatoria della competenza può essere accettata anche verbalmente purchè ci sia una successiva conferma scritta idonea a dimostrare l'esistenza dell'accordo.

È fondamentale sottolineare che laddove una delle parti del contratto è un consumatore, una sua eventuale azione nei confronti dell'altra parte *"può essere proposta davanti all'autorità giurisdizionale dello Stato membro in cui è domiciliata tale parte o, indipendentemente dal domicilio dell'altra parte, davanti alle autorità giurisdizionali del luogo in cui è domiciliato il consumatore"*[79]. Se, invece, ad essere convenuto è il consumatore, può essere adita, esclusivamente, l'autorità giudiziaria dello Stato membro nel cui territorio è domiciliato lo stesso consumatore (*cd.* foro del consumatore)[80].

Strettamente connessa all'individuazione del giudice competente è, infine, la tematica del riconoscimento e dell'esecuzione delle sentenze straniere che oggi si caratterizza per l'esistenza di uno spazio giudiziario europeo con conseguente libera circolazione delle decisioni, indipendentemente dallo specifico Paese di appartenenza del giudice adito; sarà necessario, pertanto, difendersi anche se il giudizio è instaurato all'estero ad evitare di subire, senza

[79] Così art. 18, n. 1, Regolamento 1215/12.
[80] Sul punto, v. art. 18, n. 2, Regolamento 1215/12.

aver esercitato il proprio diritto di difesa, le conseguenze scaturenti dai provvedimenti stranieri.

I principi di libera esecuzione e di pieno riconoscimento delle sentenze straniere non trovano applicazione al di fuori dell'ambito di operatività di Regolamento e Convenzione e, in ogni caso, devono essere negati, su istanza di ogni parte interessata, in tutti i casi in cui i provvedimenti stranieri: a) sono contrari all'ordine pubblico dello Stato in cui si richiede il riconoscimento[81]; b) si configura una violazione dei diritti di difesa del convenuto contumace[82]; c) sono in contrasto con una decisione già resa tra le stesse parti[83].

Può aversi contrarietà all'ordine pubblico sia in caso di violazione dei principi del giusto processo, sia quando sussistono profonde divergenze tra le disposizioni dei diversi Stati coinvolti, circostanza questa, invero, difficilmente concretizzabile nello spazio europeo attesa la tendenziale omogeneità degli ordinamenti quanto meno sotto il profilo dei principi fondamentali.

L'ipotesi di una violazione del diritto di difesa del convenuto è destinata ad avere scarsa applicazione anche in considerazione delle stesse disposizioni del Regolamento. Essa opererà nel caso in cui il convenuto non ha ricevuto regolare notifica dell'atto introduttivo del giudizio o di altro equivalente o quando, a causa del ritardo, non è stato possibile presentare tempestivamente le proprie difese. Ai sensi del Regolamento, il diritto di difesa si ritiene garantito quando il convenuto è messo concretamente nella possibilità di costituirsi e difendersi in modo adeguato a prescindere dalla regolarità formale della

[81] C*fr.* art. 45, n. 1, lett. a), Regolamento 1215/12.
[82] C*fr.* art. 45, n. 1, lett. b), Regolamento 1215/12.
[83] *Cfr.* art. 45, n. 1, lett. c e d), Regolamento 1215/12.

notifica. La presunta violazione del diritto di difesa, inoltre, non potrà essere eccepita, per opporsi al riconoscimento della sentenza straniera, quando la parte, pur avendo la possibilità, non ha impugnato il relativo provvedimento.

L'ambito su cui è intervenuto con maggior vigore il Regolamento 1215/2012 è quello del riconoscimento e dell'esecuzione delle sentenze straniere; la norma, infatti, ha abolito tutte le procedure necessarie a rendere esecutiva in uno Stato membro il provvedimento reso dall'autorità giudiziaria di altro Stato membro.

La disciplina prevista dal Regolamento 44/01 prevedeva che le decisioni emesse in uno Stato membro e ivi esecutive, potevano essere eseguite in un altro Stato membro solo dopo essere state dichiarate, dalle rispettive autorità competenti, esecutive su istanza della parte interessata.

Ai sensi del Regolamento 1215/12, invece, *"la decisione emessa in uno Stato membro che è esecutiva in tale Stato membro è altresì esecutiva negli altri Stati membri senza che sia richiesta una dichiarazione di esecutività"*[84].

È oggi possibile, pertanto, procedere all'esecuzione delle decisioni giudiziali esecutive nel territorio di uno Stato membro dell'UE anche in un altro Stato membro, procedendo semplicemente a notificare – alla parte contro cui l'esecuzione deve essere iniziata – il provvedimento ottenuto nonché l'attestato previsto dall'art. 53 del Regolamento 1215/2012[85]; entrambi i documenti devono essere opportunamente tradotti in una lingua comprensibile

[84] *Cfr.* art. 36, n. 1, Regolamento 1215/12.
[85] Sul punto, v. art. 42, Regolamento 1215/12.

alla persona contro cui è diretta l'esecuzione oppure nella lingua ufficiale dello Stato membro in cui la stessa parte è domiciliata[86].

La parte contro cui l'esecuzione è diretta ha la possibilità di presentare un'istanza all'autorità giudiziaria italiana competente per chiedere – sussistendone i presupposti previsti dal Regolamento 1215/12[87] – di negare l'esecuzione del provvedimento[88].

Dopo aver delineato le soluzioni da adottare in presenza di una controversia tra una parte italiana ed una controparte straniera domiciliata in un Paese dell'UE o dell'EFTA, è opportuno verificare come – al di fuori del campo di applicazione del Regolamento 1215/2012 e della Convenzione di Lugano – è possibile individuare, in virtù delle previsioni dell'ordinamento italiano, la giurisdizione competente.

La l. 218/95[89] prevede che il giudice italiano è competente quando *"il convenuto è domiciliato o residente in Italia o vi ha un rappresentante che sia autorizzato a stare in giudizio a norma dell'articolo 77 del codice di procedura civile e negli altri casi in cui è prevista dalla legge"*.

Pur se il convenuto non è domiciliato o residente in Italia si potrà ricorrere alla giurisdizione nazionale - sulla scorta dei criteri stabiliti dalle sezioni 2, 3 e 4 del titolo II della Convenzione di Bruxelles - quando vengano in rilievo materie comprese nel campo di applicazione della stessa Convenzione o

[86] *Cfr.* art. 43, Regolamento 1215/12.
[87] Con riferimento ai motivi di diniego del riconoscimento *cfr.* art. 45, Regolamento 1215/12.
[88] V. art. 46, Regolamento 1215/12.
[89] *Cfr.* l. 218/95, art. 3, co. 1. In particolare la norma agli artt. 3-12, reca disposizioni sulla giurisdizione mentre, agli artt. 64-71, disposizioni sul riconoscimento e l'attuazione delle sentenze e degli atti stranieri.

quando, in relazione a tutte le altre materie, la stessa giurisdizione italiana sussiste sulla base dei criteri stabiliti per la competenza per territorio.

Il richiamo alla Convenzione di Bruxelles effettuato dalla l. 218/95 comporta l'espresso riconoscimento delle disposizioni in materia di fori facoltativi e la conseguente applicazione di una disciplina uniforme, con riferimento all'individuazione della giurisdizione italiana, tanto nel caso in cui i convenuti siano domiciliati in Europa quanto nel caso in cui gli stessi si trovino in Paesi extraeuropei.

A lungo si è discusso della possibilità di estendere il richiamo fatto dalla l. 218/95 alla Convenzione di Bruxelles anche al Regolamento 44/2001 che, come precisato, ha sostituito la stessa Convenzione. L'opinione prevalente è favorevole all'applicazione estensiva del rinvio poiché se è vero che il Regolamento non può essere considerato una modificazione della Convenzione è altrettanto vero che lo stesso è il suo naturale sostituto[90].

L'art. 4, co. 1, l. 218/95 disciplina le ipotesi di accettazione e deroga della giurisdizione italiana.

Quest'ultima può essere convenzionalmente individuata, per iscritto, pur se la sua applicazione non scaturisce dall'art. 3 e, inoltre, è accettata per fatti concludenti del convenuto quando quest'ultimo, comparendo in giudizio, non eccepisce l'eventuale difetto di giurisdizione nel suo primo scritto difensivo.

È anche possibile, come anticipato, derogare la competenza del giudice italiano a vantaggio di un giudice straniero o di un arbitro estero, purché la

[90] In termini, v. M. A. LUPOI, *Conflitti transnazionali di giurisdizioni,* II vol., Milano, 2002, p. 316.

deroga sia provata per iscritto e non sia relativa a diritti disponibili. La forma scritta è richiesta *ad probationem* e la deroga non sarà efficace quando il giudice o gli arbitri incaricati *"declinano la giurisdizione o comunque non possono conoscere della causa"*[91]; in tal caso la domanda può essere proposta al giudice italiano anche in presenza di un eventuale provvedimento con cui è stata riconosciuta l'efficacia dell'accordo di deroga.

Non vi è dubbio che la disciplina dettata dalla l. 218/95, in merito alla validità della deroga, produce i suoi effetti nell'ambito dell'ordinamento italiano e non anche in quello di appartenenza della controparte contrattuale.

Perché ciò accada, infatti, è necessario, che – in assenza di un trattato bilaterale – l'ordinamento del Paese estero riconosca validità a clausole attributive di competenza a giudici stranieri.

Dall'applicazione della l. 218/95 sono scaturite importanti novità anche in merito al riconoscimento dei provvedimenti stranieri; ai sensi dell'art. 64, infatti, la sentenza è riconosciuta in Italia senza che sia necessaria alcuna procedura di recepimento in tutti i casi in cui *"a) il giudice che l'ha pronunciata poteva conoscere della causa secondo i princìpi sulla competenza giurisdizionale propri dell'ordinamento italiano; b) l'atto introduttivo del giudizio è stato portato a conoscenza del convenuto in conformità a quanto previsto dalla legge del luogo dove si è svolto il processo e non sono stati violati i diritti essenziali della difesa; c) le parti si sono costituite in giudizio secondo la legge del luogo dove si è svolto il processo o la contumacia è stata dichiarata in conformità a tale legge; d) essa è passata in giudicato secondo la*

[91] V. art. 4, co. 3, l. 218/95.

legge del luogo in cui è stata pronunziata; e) essa non è contraria ad altra sentenza pronunziata da un giudice italiano passata in giudicato; f) non pende un processo davanti a un giudice italiano per il medesimo oggetto e fra le stesse parti, che abbia avuto inizio prima del processo straniero; g) le sue disposizioni non producono effetti contrari all'ordine pubblico".

Il nuovo approccio ha determinato un'evidente riduzione delle ipotesi in cui è possibile impedire il riconoscimento in Italia di un provvedimento estero.

Ciò, invero, accadrà in tutti i casi in cui si pone in essere una lesione di fondamentali garanzie sostanziali e processuali quali sono, ad esempio, il diritto di difesa e la necessità di conoscenza dell'atto introduttivo del giudizio da parte del convenuto sulla scorta delle disposizioni del Paese in cui si è svolto il giudizio.

La pronuncia straniera, inoltre, per essere riconosciuta, non dovrà determinare una lesione dei principi posti a garanzia dell'ordine pubblico e dovrà essere emessa da un giudice che *"poteva conoscere della causa secondo i principi sulla competenza giurisdizionale propri dell'ordinamento italiano"*.

L'ulteriore recepimento delle sentenze straniere potrà avvenire, infine, in ragione di convenzioni bilaterali che possono determinare le modalità di recepimento in entrambi i Paesi ed i suoi presupposti.

6.- *Dalle Alternative Dispute Resolution alle Online Dispute Resolution.*

Per completare il quadro dei rimedi esperibili in caso di controversie relative, in generale, ai contratti internazionali ed, in particolare, ai contratti di *cloud computing*, è opportuno richiamare, sia pur in considerazione di

un'operatività circoscritta al territorio Europeo, la Direttiva UE 2013/11 sulla risoluzione alternativa delle controversie con i consumatori ed il Regolamento 524/2013 sulle procedure di *online dispute resolution*.

La Direttiva 2013/11 è stata emanata con l'obiettivo di introdurre regole e procedure per garantire ai consumatori la possibilità di attivare, su base volontaria, procedimenti stragiudiziali – gestiti da organismi ADR qualificati – per risolvere eventuali controversie sorte a seguito della sottoscrizione di contratti di vendita di beni o servizi[92].

La Direttiva mira a fornire un quadro unitario utile a disciplinare la risoluzione stragiudiziale delle controversie concernenti le obbligazioni contrattuali – derivanti da contratti di vendita o servizi – sorte, come già precisato, tra consumatori residenti nell'Unione Europea e professionisti stabiliti nella stessa Unione, sia quando il consumatore ed il professionista risiedono e sono stabiliti nello stesso Stato membro, sia quando risiedono e sono stabiliti in Stati membri diversi.

La gestione delle controversie dovrà essere affidata ad un organismo ADR *"che propone o impone una soluzione o riunisce le parti al fine di agevolare una soluzione amichevole"*[93].

Si deve precisare che la Direttiva ADR non si applica alla gestione interna dei reclami dei consumatori gestiti dal professionista, alle controversie fra

[92] La Direttiva *cd.* ADR precisa che per "contratto di vendita" si intende qualsiasi contratto in base al quale il professionista trasferisce o si impegna a trasferire la proprietà di beni al consumatore e il consumatore ne paga o si impegna a pagarne il prezzo; per "contratto di servizi", invece, si intende qualsiasi contratto diverso da un contratto di vendita in base al quale il professionista fornisce o si impegna a fornire un servizio al consumatore e il consumatore ne paga o si impegna a pagarne il prezzo.
[93] V. art. 2, Direttiva 2013/11/UE.

professionisti, agli eventuali tentativi di composizione della controversia posti in essere da un giudice nell'ambito di un procedimento giudiziario riguardante la controversia stessa, ai servizi di assistenza sanitaria, agli organismi pubblici di istruzione superiore o di formazione continua ed infine, essendo uno strumento pensato per il "consumatore", alle procedure avviate da un professionista proprio nei confronti di un consumatore.

Gli organismi ADR – che sono abilitati se in possesso dei requisiti richiesti dal legislatore – devono operare in modo efficace, equo, indipendente e trasparente garantendo idonei *standard* di qualità.

Gli operatori commerciali che decidono di far uso di una procedura ADR, o sono obbligati a tanto, devono informare i consumatori sia utilizzando il proprio sito *web* sia integrando i termini e le condizioni generali di vendita dei beni o dei servizi proposti.

La durata massima di un procedimento di risoluzione alternativa della controversia non può superare i 90 giorni; i conciliatori devono essere terzi e imparziali rispetto alle parti in contesa e l'accesso alla procedura dovrà essere gratuito o, al più, soggetto ad un versamento simbolico.

Il d.lgs. 28/10 che disciplina nell'ordinamento italiano l'istituto della mediazione è un chiaro esempio di provvedimento coerente con il contenuto ed i principi propri della Direttiva 2013/11/UE.

Al Regolamento 524/2013/UE, noto anche come Regolamento ODR e da coordinare con la predetta Direttiva, si deve l'introduzione nell'ordinamento europeo delle *on line dispute resolution* (ODR) basate sull'utilizzo di un'unica piattaforma elettronica europea.

Il Regolamento ODR – che, data la sua natura, non necessita di recepimento – si applica alla risoluzione extragiudiziale delle controversie concernenti obbligazioni contrattuali, derivanti da contratti di vendita di beni o di servizi *online*[94], tra un consumatore residente nell'Unione e un professionista stabilito nell'Unione.

La gestione della lite, demandata ad un organismo ADR inserito in elenco di soggetti abilitati, è gestita su di un'apposita piattaforma elettronica e a distanza.

Il Regolamento ODR, a differenza di quanto previsto dalla Direttiva ADR, trova applicazione anche per la risoluzione extragiudiziale delle controversie concernenti obbligazioni contrattuali, derivanti da contratti di vendita o di servizi *online*, avviate da un professionista nei confronti di un consumatore sempre che la legislazione dello Stato membro cui appartiene il consumatore, consenta l'intervento di un organismo ADR.

La piattaforma UE[95], disponibile in tutte le lingue ufficiali dell'Unione Europea, consente la presentazione *online* della richiesta di avvio della procedura all'organismo ADR individuato; il reclamo "telematico" potrà essere presentato dal consumatore che riscontra problemi a seguito di un acquisto *online*.

---

[94] Il Regolamento 524/2013/UE definisce il "contratto di vendita o di servizi *online*" come il contratto di vendita o di servizi in base al quale il professionista, o l'intermediario del professionista, offre beni o servizi mediante un sito *web* o altri mezzi elettronici e il consumatore effettua l'ordinazione di tali beni o servizi su tale sito *web* o mediante altri mezzi elettronici.

[95] La piattaforma UE e reperibile all'indirizzo *https://webgate.ec.europa.eu/odr/main/?event= main.home.show&lng =IT*.

La piattaforma ODR, preso in carico il reclamo, comunicherà automaticamente, al venditore del bene o al fornitore del servizio *on line*, che è stata presentata una recriminazione contro di lui.

Le parti, quindi, entro trenta giorni[96], individueranno l'organismo ADR nazionale a cui rivolgersi per provare a definire la loro controversia. Tutti gli elementi relativi alla stessa controversia, utili alla sua definizione, saranno trasmessi per il tramite della piattaforma ODR collegata agli organismi ADR nazionali.

[96] In caso di mancato accordo nel termine di trenta giorni il reclamo *online* non può essere presentato.

Capitolo III
Il contratto di *cloud computing*

SOMMARIO: 1. *Cloud computing*, *point and click* e tutela della parte contrattualmente debole; 2. La struttura del contratto di *cloud computing*; 3. La qualificazione giuridica del contratto di *cloud computing*; 3.1. (segue) Il contratto di *cloud computing* come somministrazione di servizi; 4. Il contratto di *cloud computing* come contratto misto; 5. Il *cloud computing* e la standardizzazione delle clausole contrattuali; 6. Il contratto di *cloud computing* e l'abuso di dipendenza economica nei rapporti B2b.

1.- *Cloud computing, point and click e tutela della parte contrattualmente debole.*

Dopo aver affrontato le questioni relative all'individuazione della legge applicabile al contratto di *cloud computing*, sempre più caratterizzato da elementi di internazionalità, nonché quelle attinenti l'individuazione del giudice competente a risolvere eventuali controversie scaturenti dalla sua esecuzione, è opportuno soffermarsi sull'approccio che il diritto interno ha nei confronti dello stesso contratto.

Come si è già avuto modo di precisare, la stipula dei contratti di *cloud computing*, nella quasi totalità dei casi, non contempla la fase trattativa poiché la conclusione avviene *on line* tramite l'adesione a moduli e formulari predisposti unilateralmente dai *cloud provider*. Tale modalità di raggiungimento dell'accordo riduce il potere contrattuale dell'utente che si

limita a dover valutare l'opportunità o meno di aderire alle offerte predisposte dal fornitore. Lo squilibrio tra le parti contrattuali raggiunge, sicuramente, il suo apice quando le clausole contrattuali predisposte unilateralmente dal fornitore del servizio sono vessatorie[97] e quando oggetto dell'offerta sono i servizi rientranti nel cd. *public cloud* poiché, in tal caso, qualsiasi ipotesi di contrattazione è da escludere completamente.

Nel nostro ordinamento tale modalità di raggiungimento dell'accordo rientra nel *genus* dei contratti per adesione conclusi, fuori dei locali commerciali, mediante l'utilizzo di strumenti informatici.

Il *cloud provider*, attraverso la conclusione *cd. point and click*, predispone sul *web* la propria offerta commerciale precisando l'esatto contenuto dell'accordo negoziale; conseguentemente, la pressione del tasto negoziale, configurabile come un comportamento concludente, determina l'accettazione per *facta concludentia* valida ed efficace in tutti i casi in cui i contratti sono a forma libera.

Tale modalità di conclusione di contratto, ai fini della sua validità, deve essere necessariamente coordinata con la disciplina protettiva della cd. parte contrattualmente debole contenuta, essenzialmente, negli artt. 1341 e 1342 c.c. e nel Codice del Consumo[98].

In particolare, al fine di valutare la validità delle clausole contrattuali con specifico riferimento al contraente debole, è opportuno distinguere i casi in cui

[97] Si considerino, ad esempio, le clausole con cui è previsto la riduzione della responsabilità o, addirittura, l'esonero dalla stessa responsabilità per il *cloud provider* in presenza di danni, perdite o accessi di terzi ai dati archiviati. Si pensi, inoltre, a quelle clausole che comportano una limitazione della possibilità di recedere dal contratto o, ancora, alla deroga del cd. foro del consumatore.

[98] D.lgs. 06.09.05, n. 206, Codice del consumo.

l'utente dei servizi *cloud* è un "consumatore" rispetto a quelli in cui è un "professionista".

Se l'utente *cloud* è un consumatore avranno sicuro rilievo le disposizioni del Codice del consumo contenute negli articoli da 33 a 38 tese a limitare l'autonomia contrattuale del professionista per evitare eventuali abusi a danno del consumatore.

Il legislatore ha individuato una serie di clausole che si presumono vessatorie fino a prova contraria[99]; in particolare, l'art. 33 statuisce che *"[...] si considerano vessatorie le clausole che, malgrado la buona fede*[100]*, determinano a carico del consumatore un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto"* elencando, poi, le clausole ritenute abusive in via presuntiva. Si tratta, invero, di una presunzione non assoluta che il professionista può superare dimostrando che l'assetto contrattuale, nel suo complesso, non determina uno squilibrio a danno del consumatore.

L'art. 36, d.lgs. 206/05, invece, ha previsto una *"praesumptio iuris et de iure"* che, come tale, non ammette una prova contraria per quelle clausole che, pur se frutto di un'eventuale trattativa individuale, hanno per oggetto o per effetto di: *"a) escludere o limitare la responsabilità del professionista in caso di morte o danno alla persona del consumatore, risultante da un fatto o da un'omissione del professionista; b) escludere o limitare le azioni del consumatore nei confronti del professionista o di un'altra parte in caso di*

[99] Sul punto, v. E. BELISARIO, *cit.*, p. 15 ss.
[100] Il rinvio al concetto di buona fede deve essere valutato in senso soggettivo come l'"ignoranza" del professionista di ledere un altrui diritto. In altre parole, la tutela prevista dal legislatore opera a vantaggio della parte debole a prescindere dall'eventuale mala fede del professionista.

inadempimento totale o parziale o di adempimento inesatto da parte del professionista; c) prevedere l'adesione del consumatore come estesa a clausole che non ha avuto, di fatto, la possibilità di conoscere prima della conclusione del contratto".

La presenza in un contratto di *cloud computing* di suddette clausole comporta la nullità delle stesse; si tratta di una nullità relativa, operando solo a vantaggio del consumatore, e parziale, restando valido il contratto in tutte le restanti parti. La nullità potrà essere rilevata anche d'ufficio senza la necessità di una specifica impugnazione da parte del consumatore.

La nullità delle clausole – ad eccezione di quelle previste dall'art. 36, d.lgs. 206/05 – potrà essere evitata se è possibile provare che le stesse sono oggetto di una specifica trattativa individuale; ciò, relativamente ai contratti di *cloud computing*, è quasi impossibile poiché, come anticipato, gli stessi difficilmente sono oggetto di una negoziazione e di una trattativa individuale; l'utilizzo del modello dell'adesione comporta, inoltre, il venire meno della stessa sottoscrizione sostituita dal comportamento concludente rappresentato dalla pressione del tasto negoziale.

Se il *cloud consumer* è un professionista, si deve guardare alla disciplina dettata dagli artt. 1341 e 1342 cc. in materia di condizioni generali di contratto e di contratti conclusi mediante moduli o formulari. Pur trattandosi della modalità con cui tipicamente sono stipulati *on-line* i contratti di *cloud computing*, non sono poche le problematiche applicative scaturenti dalle predette disposizioni.

Ai sensi dell'art. 1341 c.c. le condizioni generali di contratto sono efficaci nei confronti dell'altra parte che non le ha predisposte se *"al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle usando l'ordinaria diligenza*.

In ogni caso non hanno effetto, se non sono specificamente approvate per iscritto, le condizioni che stabiliscono, a favore di colui che le ha predisposte, limitazioni di responsabilità, facoltà di recedere dal contratto o di sospenderne l'esecuzione, ovvero sanciscono a carico dell'altro contraente decadenze, limitazioni alla facoltà di opporre eccezioni, restrizioni alla libertà contrattuale nei rapporti coi terzi, tacita proroga o rinnovazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziaria". Il legislatore, anche in questo caso, ha privilegiato l'interesse della controparte, che non ha inciso sulla predisposizione del regolamento contrattuale, richiedendo una specifica "approvazione scritta" a significare una piena cognizione della previsione contrattuale.

L'approvazione scritta necessaria per riconoscere l'efficacia delle clausole vessatorie, mal si concilia con l'adesione per *facta concludentia* fatte salve le ipotesi in cui non è richiesta la specifica approvazione[101] e le ipotesi in cui il tasto negoziale è sostituito, nel modulo *online*, dall'utilizzo di una firma elettronica qualificata in grado di garantire gli effetti propri della sottoscrizione autografa.

[101] Si pensi, ad esempio, ai *cd.* negozi *per relationem* che fanno riferimento ad un separato documento nel quale sono riportate le stesse clausole vessatorie specificamente approvate.

Alla luce di quanto sino ad ora precisato, quindi, le clausole vessatorie contenute in un contratto telematico di *cloud computing* sono inefficaci a meno che non si proceda alla loro sottoscrizione su documenti cartacei collegati a quelli elettronici.

L'art. 1342 c.c. disciplina le ipotesi di contratti conclusi mediante la sottoscrizione di moduli o formulari *"predisposti per disciplinare in maniera uniforme determinati rapporti"*. Le clausole aggiunte al modulo o al formulario, ferma restando la previsione di cui all'art. 1341 c.c., prevalgono su quelle originali laddove sono con esse incompatibili. In un contratto telematico di *cloud computing*, invero, sarà difficile distinguere le clausole originarie da quelle successivamente aggiunte a meno che non siano adottati opportuni accorgimenti tecnologici.

Nella remota ipotesi in cui si dovesse giungere alla conclusione di un contratto di *cloud computing* all'esito di una seppur minima trattativa individuale, si potrà ipotizzare – in alternativa ad stipula tradizionale comunque possibile anche nel caso di accettazione della proposta mediante adesione – uno scambio di proposta ed accettazione tramite posta elettronica.

In ipotesi residuali sarà possibile, inoltre, addivenire ad un accordo anche in forza di quanto previsto dall'art. 1327 c.c. secondo cui *"il contratto è concluso nel tempo e nel luogo in cui ha avuto inizio l'esecuzione"*[102]. Si tratta di una modalità di conclusione che si avvicina molto a quella per comportamenti

[102] Un tipico esempio di contratto concluso contestualmente alla sua esecuzione è quello che si caratterizza per transazioni, aventi ad oggetto beni o servizi, basate sul pagamento tramite carta di credito laddove il trasferimento dei fondi costituisce atto di esecuzione con riferimento all'adempimento dell'obbligazione pecuniaria.

concludenti, discostandosi, al contempo, dallo schema ordinario dello scambio proposta/accettazione.

2.- *La struttura del contratto di cloud computing.*

Il contratto di *cloud computing* assume un ruolo fondamentale nella definizione degli obblighi in capo alle parti, regolando le modalità con cui devono essere resi i servizi *cloud*[103]. Con tale contratto si instaura un rapporto giuridico in ragione del quale il *provider* offre all'utente, mediante accesso remoto, i servizi *cloud* già individuati nella prima parte di questo lavoro.

Prestazione caratteristica del contratto di *cloud computing* è sicuramente l'erogazione di un servizio; ciò emerge, in tutta evidenza, dalla stessa denominazione delle varie tipologie di *cloud* caratterizzate dalla locuzione *as service* (*software as service*, *platform as service*, *infrastructure as service*).

Si tratta di un aspetto giuridicamente rilevante poiché la tecnologia *cloud* ha determinato il passaggio da un modello cd. proprietario, basato su l'acquisto delle risorse informatiche con conseguente controllo diretto delle stesse, ad un modello basato sull'accesso ad uno o più servizi informatici messi a disposizione da terzi fornitori. L'utente *cloud* non ha più una relazione diretta con il sistema informatico ma, sfruttando le potenzialità di *internet*, può accedere alle risorse messe a disposizione dal *provider* che, a sua volta, deve garantire il funzionamento dei sistemi secondo gli *strandard* contrattualmente

[103] Sulla natura di servizio delle prestazioni cui si obbliga il fornitore v. S. BRADSHAW, C. MILLARD, I. WALDEN, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, in *International Journal of Law and Information Technology*, 2011, p. 187.

definiti[104]. Non è importante, quindi, essere proprietari della risorsa ma, piuttosto, essere posti nella condizione di accedere alla tecnologia detenuta ed erogata da terzi in linea con la cd. "cultura dell'accesso"[105]. In quest'ottica ed in considerazione della necessaria continuità delle prestazioni, a garanzia della fruibilità delle risorse informatiche, è fondamentale la puntuale regolamentazione del rapporto contrattuale.

I contratti di *cloud computing*, sotto un profilo strutturale, sono generalmente composti da quattro diversi documenti recanti, rispettivamente, le condizioni generali di contratto, i livelli qualitativi dei servizi, gli obblighi comportamentali assunti dalle parti ed infine le modalità di trattamento dei dati personali[106].

Le condizioni generali di contratto, indicate anche con l'acronimo CGC in alternativa a ToS (*terms of service*), definiscono le modalità con cui sarà offerto il servizio ricomprendendo elementi essenziali quali la durata del vincolo contrattuale, il corrispettivo da versare, l'individuazione delle ipotesi di risoluzione e di recesso nonché della legge e della giurisdizione applicabili.

---

[104] Sull'idea dell'informatica come servizio e non come bene, v. D.F. PARKHILL, *The Challenge of the Computer Utility*, Londra, 1966.

[105] Sul tema della cultura dell'accesso basato sulla garanzia della disponibilità temporanea di beni o servizi, v. J. RIFKIN, *L'era dell'accesso*. *La rivoluzione della new economy* Milano, 2000 nonché, con specifico riferimento al *cloud computing*, SUN MICROSYSTEMS, *Introduction to the Cloud Computing Architecture, White Paper, 1st Edition*, giugno 2009, in *http://webobjects.cdw.com*; INTERNATIONAL TELECOMMUNICATION UNION, *Distributed Computing: Utilities, Grid & Clouds*, 2009, in *www.itu.int*. Sul nuovo approccio giuridico scaturente dalla "cultura dell'accesso" v. A. STAZI, *"Marketplace of ideas" e "accesso pluralistico" tra petizioni di principio e ius positum*, in *Dir. informazione e informatica*, 2009, p. 635 ss.

[106] Per un'analisi dei modelli contrattuali adottati da quattro tra i principali fornitori dei servizi di *cloud computing*, v. l'indagine condotta dalla *Queen Mary University of London*, *School of law*, in S. BRADSHAW, C. MILLARD, I. WALDEN, *cit.*
La valutazione della struttura del contratto di *cloud computing* scaturisce dall'analisi dei contratti adottati dai principali fornitori di servizi *cloud* oggetto di indagine.

I livelli qualitativi e quantitativi dei servizi offerti dal fornitore in ragione del prezzo versato, sono indicati e regolati dal documento ormai comunemente conosciuto come *Service Level Agreement* (SLA). Con l'*Acceptable Use Policy* (AUP), invece, si è soliti definire le ipotesi in cui il *provider* è legittimato a sospendere o interrompere l'erogazione del servizio a seguito di un utilizzo dell'*hardware* e del *software*, a disposizione dell'utente, non conforme agli usi consentiti indicati nello stesso AUP.

La *privacy policy*, infine, descrivendo le modalità di trattamento dei dati che confluiscono nel sistema *cloud*, è l'ultimo documento che compone il contratto.

Come già ampiamente illustrato, il contratto di *cloud computing* è costruito, nella quasi totalità dei casi, sulla base del modello "uno a molti" con conseguente standardizzazione della contrattazione ad opera del *provider* che, in quasi assoluta autonomia, definisce il contenuto dei citati documenti e, quindi, del contratto globalmente inteso.

Nel quadro così delineato è evidente che il contratto di *cloud computing*, si presta, forse più di altri contratti, ad essere soggetto ad alterazioni funzionali; un ruolo centrale è sicuramente rivestito dal *Service Level Agreement* (SLA) che, definendo le caratteristiche del servizio contrattualizzato, consente di circoscrivere con precisione l'oggetto del contratto con specifico riferimento ai parametri tecnici, oggettivi e misurabili, importanti indicatori dell'effettivo livello qualitativo del servizio offerto[107]. In altre parole, il *Service Level*

[107] Si considerino, ad esempio, i tempi di *uptime* corrispondenti all'arco temporale in cui un qualsiasi elaboratore informatico è acceso ed operativo ed i tempi di *downtime* in cui, invece, l'elaboratore non è funzionante per un guasto o per manutenzione. Anche il *cd.* tempo di latenza è sicuramente da ricomprendere tra i parametri tecnici integrabili nel SLA individuando la velocità di risposta di un sistema a determinati *input*.

Agreement consente di verificare la conformità della prestazione erogata dal *provider* al regolamento contrattuale; dalla combinazione tra i livelli di servizio promessi e le conseguenze previste per la violazione di quanto contrattualmente definito, emergono parametri fondamentali per definire la responsabilità contrattuale per inadempimento del *cloud provider*.

Come rilevato, inoltre, i *cloud provider* hanno imposto termini e condizioni generali di contratto non solo nell'ambito di rapporti B2C, caratterizzati dalla presenza di un consumatore debole, ma anche nei rapporti B2B intercorrenti tra professionisti. Il *provider*, infatti, anche in tale circostanza riesce a predisporre in quasi completa autonomia documenti contrattuali in base ai quali il servizio viene fornito "*as it is*"[108] con la previsione, nelle stesse CGC, di clausole di esonero della responsabilità che finiscono con il vanificare le funzioni e le garanzie che dovrebbero scaturire dall'adozione dei *Service Level Agreement*.

Spesso accade che questi ultimi non indicano con precisione i parametri di riferimento limitandosi a specificare un livello massimo e minimo del servizio offerto. Il livello minimo, invero, sarà il reale parametro a cui si dovrà guardare per rilevare l'eventuale inadempimento del *provider* che, di contro, considererà il livello massimo una semplice meta da raggiungere.

In presenza di SLA effettivi e non meramente indicativi, è spesso previsto un indennizzo, a ristoro dell'eventuale indisponibilità del servizio, basato, alternativamente, sul riconoscimento di crediti in fattura o sull'estensione della

[108] V. WIEDER, BUTLER, THEILMANN, YAHYAPOUR (a cura di), *Service Level Agreements for Cloud Computing,* Londra, 2011.

durata dello stesso servizio[109]. Il *cloud provider*, in questo modo, tenta di forfettizzare l'eventuale danno arrecato all'utente che, a sua volta - in considerazione della propria attività e delle ricadute negative scaturenti dalla sospensione od interruzione del servizio contrattualizzato - dovrà opportunamente valutare il rischio di un eventuale inadempimento e l'idoneità del ristoro offerto, a coprire danni subiti sia diretti che indiretti.

3.- *La qualificazione giuridica del contratto di cloud computing.*

L'interesse per una gestione decentralizzata, delocalizzata, continuativa e condivisa di risorse informatiche e documenti digitali costituisce la causa del contratto di *cloud computing* in linea con i parametri di liceità e meritevolezza sanciti, rispettivamente, dagli artt. 1343 e 1322 c.c.

L'oggetto del contratto, invece, può essere individuato nell'accesso remoto ad una serie di risorse informatiche opportunamente configurate per rendere una molteplicità di servizi. Come visto, a fronte dell'obbligo dell'utente di pagare un prezzo per la fruizione, per fini leciti, dei servizi a lui necessari, è previsto il corrispondente obbligo del *cloud provider* di consentire un accesso scalabile, anche alternativo, ai servizi IaaS, PaaS e SaaS garantendo il funzionamento dei sistemi informatici e la disponibilità di spazio *hosting* con conseguente messa in sicurezza dei dati archiviati.

Laddove le parti, all'atto della stipula, non circoscrivono analiticamente l'oggetto del contratto, lo stesso potrà essere determinato sulla scorta delle

[109] Sul punto, v. G. RIZZO, *La Responsabilità contrattuale nella gestione dei dati nel cloud computing*, in *Diritto Mercato Tecnologia*, 2013, p. 102.

concrete esigenze dell'utente senza che da questa decisione unilaterale possa scaturire un'inammissibilità della scelta[110]; nel caso di specie, infatti, come accade nell'ipotesi prevista dall'art. 1560, n. 2, c.c., la determinazione è effettuata dalla parte contrattualmente più debole e per ragioni connesse alle modalità di erogazione del servizio in assenza di effetti lesivi per la controparte.

Fino ad ora, nonostante la notevole diffusione della tecnologia *cloud* non è stato possibile giungere ad un'unitaria qualificazione giuridica del contratto di fornitura dei servizi *cloud*; le soluzioni proposte, infatti, sono molteplici e si dividono tra quelle che lo riconducono allo schema negoziale tipico del contratto di appalto di servizi e all'*outsourcing* nonchè quelle che rinviano alla figura del contratto di licenza d'uso o del contratto di locazione.

La tesi che riconduce il contratto di *cloud computing* allo schema dell'appalto di servizi, sembra essere quella più seguita ma non la più convincente ritenendo, invece, da preferire la riferibilità dello stesso contratto di *cloud* alla somministrazione di servizi. Invero, considerando che gli accordi di *cloud computing* si caratterizzano spesso per l'alternanza di previsioni riferibili a diversi tipi contrattuali non consentendo, di fatto, la prevalenza di un profilo contrattuale su di un altro, è opportuno, in tali circostanze, inquadrarli come contratti misti[111] in cui si combinano prestazioni caratteristiche di diversi tipi legali.

---

[110] Sulle modalità di determinazione dell'oggetto del contratto, *cfr.* V. ROPPO, *Il contratto*, in *Trattato di Diritto Privato*, IUDICA, ZATTI (a cura di), Milano, 2001, p. 355 ss.

[111] Alcuni autori hanno tentato di ricondurre il contratto di *cloud computing* nel novero dei cd. contratti prettamente atipici escludendo qualsiasi sussunzione del negozio nell'ambito dei riferiti schemi tipici. Sul punto, v. N. FABIANO, *I nuovi paradigmi della rete. Distribueted*

L'art. 1655 c.c. definisce l'appalto come il contratto con cui l'appaltatore assume, dietro corrispettivo, con l'organizzazione dei mezzi necessari e con la gestione a proprio rischio, il compimento di un'opera o di un servizio con la conseguente assunzione di un'obbligazione di risultato.

Come è stato opportunamente sottolineato[112] l'appalto di servizi ha ad oggetto la *"produzione di un'utilità senza elaborazione e trasformazione di materie"*[113] a differenza dell'appalto d'opera che si caratterizza per la *"modificazione dello stato materiale di cose preesistenti"*[114]. Si può parlare, in ogni caso, di appalto di servizi anche quando l'obbligo dell'appaltatore di dar corso ad una modifica materiale costituisce esclusivamente un elemento accessorio e funzionale al conseguimento di un diverso scopo principale.

L'appalto di servizi, pertanto, consiste in un *facere* che nel contratto di *cloud computing* viene individuato nella messa a disposizione di una struttura informatica esterna rispetto agli utenti che, per il suo tramite, potranno fruire di servizi gestiti da terzi.

---

computing, cloud computing e "computing paradigms": abstract sugli aspetti e i profili giuridici, in *http://www.diritto.it/docs/27973-i-nuovi-paradigmi-della-rete-distribueted-computing-cloud-computing-e-computing-paradigms-abstract-sugli-aspetti-e-i-profiligiuridici?Page=2*. Non condividendo la strada tracciata, è opportuno ricordare quanto sostenuto autorevolmente da V. ROPPO, *Introduzione*, in *Trattato della responsabilità contrattuale*, VISENTINI (a cura di), Padova, 2009, p. 4, secondo cui un simile inquadramento non risponde all'esigenza di definire il quadro normativo da cui desumere i diritti e gli obblighi che scaturiscono dal contratto tra le parti.

[112] V. M. STOLFI, *Appalto (contratto di)*, in *Enciclopedia del Diritto*, Milano, 1958, p. 647; D. RUBINO, *Dell'appalto*, in *Commentario del codice civile*, A. SCIALOJA, G. BRANCA (a cura di), Bologna, 1973, p. 25; C. GIANNATTASIO, *L'appalto*, Milano, 1977, p. 102.

[113] D. RUBINO, *L'appalto*, Torino, 1980, p. 137. Sul punto, v. anche Cass. 17.04.2001, n. 5609, in *Giust. civ.*, 2001, I, 2963 secondo cui *"la distinzione tra appalto d'opera e appalto di servizi riguarda l'oggetto del contratto che può consistere sia in opere che in servizi, intendendosi per opera qualsiasi modificazione dello stato materiale di cose preesistenti e per servizio qualsiasi utilità che può essere creata da un altro soggetto, diversa dalle opere; la qualificazione del contratto come appalto d'opera o come appalto di servizi costituisce accertamento di fatto riservato al giudice del merito ed insindacabile in sede di legittimità, se congruamente motivato*"; V., inoltre, Cass. 04.12.1997, n. 12304, in *Giur. it.*, 1998, 2066.

[114] D. RUBINO, *ibidem*.

La maggior parte delle disposizioni dettate dal codice civile in materia di appalto sono dedicate all'appalto d'opera laddove l'appalto di servizi risulta menzionato esclusivamente nelle norme relative alla definizione di appalto (art. 1655 c.c.), al subappalto (art. 1656 c.c.), al recesso (art. 1671 c.c.) e ai sevizi continuativi (art. 1777 c.c.). Invero, come riconosciuto dalla stessa giurisprudenza di legittimità, all'appalto di servizi possono applicarsi le norme previste per l'appalto d'opera poiché *"l'applicabilità delle singole norme via via dettate per l'appalto d'opera e appalto di servizi non deriva dal riferimento delle stesse all'uno o all'altro, bensì alla loro compatibilità o incompatibilità con il contenuto specifico del rapporto"*[115]. Conseguentemente sono da ritenere incompatibili con l'appalto di servizi l'art. 1658 c.c. in tema di fornitura della materia, l'art. 1663 c.c. relativo alla denuncia dei difetti della stessa materia da parte dell'appaltatore, l'art. 1669 c.c. sulla rovina e sui difetti di cose immobili ed infine l'art. 1673 relativo al perimento o al deterioramento dell'opera prima della consegna.

Sarano sicuramente applicabili, invece, le previsioni in tema di variazioni (artt. 1660 e 1661 c.c.), di revisione dei prezzi (art. 1664 c.c.), di verifiche in corso d'opera (art. 1662 c.c.), di garanzie (artt. 1667 e 1668 c.c.) e di recesso (art. 1671 c.c.).

Sovente, a sostegno della riconducibilità del contratto di *cloud computing* alla disciplina dell'appalto di servizi, viene posta, in linea con l'art. 1655 c.c., la presenza di un'organizzazione d'impresa in grado di gestire le esigenze degli

[115] Cass. 21.05.83, n. 3530, in *Rep. Foro it.*, 1983, Appalto [0430], n. 104.

utenti del *cloud* che richiedono i servizi informatici erogati dai *cloud provider*[116].

Questi ultimi, a loro volta, nell'ottica tracciata dallo stesso art. 1655 c.c., assumono il rischio contrattuale scaturente dalla gestione della struttura informatica a disposizione degli utenti rispondendo per l'eventuale inadempimento contrattuale.

L'appalto di servizi presenta caratteristiche che, indubbiamente, ben si attagliano alla figura negoziale del *cloud computing* anche se è opportuno evidenziare alcuni elementi di divergenza costituiti dalla possibile gratuità del *cloud* rispetto al carattere corrispettivo dell'appalto nonché dall'impossibilità per l'utente *cloud*, in ragione della standardizzazione delle offerte, di scegliere e di determinare le caratteristiche dei servizi richiesti a differenza di quanto accade con l'appalto che garantisce al committente un elevato livello di personalizzazione.

Il contratto di *cloud computing*, come anticipato, è spesso associato al cd. *outsourcing* soprattutto in considerazione della diffusione e del grande utilizzo della tecnologia *cloud* nell'ambito di rapporti B2B intercorrenti tra *cloud provider* ed aziende.

Con il termine *outsourcing* non si individua uno specifico ed autonomo tipo negoziale ma, piuttosto, ci si riferisce ad una particolare modalità di organizzazione aziendale[117] basata sull'affidamento di alcune attività

---

[116] Sul punto, v. E. BELISARIO, *op. cit.*

[117] V. F. CARDARELLI, *La cooperazione tra imprese nella gestione di risorse informatiche: aspetti giuridici del cd. "outsourcing"*, in *Dir. informazione e informatica*, 1993, p. 85 ss.; M. PITTALIS, *Outsourcing*, in *Contratto e impr.*, 2000, p. 1006 ss.

produttive a soggetti terzi esterni all'azienda e ad essa non appartenenti[118] fatte salve le ipotesi in cui il modello dell'*outsourcing* si realizza ricorrendo a società specializzate appartenenti allo stesso gruppo dell'*outsourcer*.

In altri casi, invece, imprese autonome, unificando proprie strutture specializzate, possono costituire dei veri e propri *"group outsourcing"* cui sono affidate determinate attività[119]. Queste strutture, inoltre, in presenza di un elevato grado di qualificazione, possono addirittura aprirsi all'esterno offrendo i loro servizi sul mercato sviluppando, così, un autonomo *business*.

Il ricorso all'*outsourcing* è il frutto di esigenze differenti costituite dalla possibilità di: a) evitare gravosi investimenti scaturenti da determinate attività; b) risolvere il problema dell'aggiornamento tanto delle risorse umane quanto di quelle tecnologiche; c) ridurre sensibilmente i costi aziendali incrementando, al contempo, l'efficienza produttiva grazie all'impiego della specializzazione del fornitore; d) poter essere immediatamente competitivi rispondendo alle esigenze del mercato senza dover dar corso a gravosi processi di adeguamento interno.

Sotto un profilo strettamente giuridico l'*outsourcing*, non costituendo una tipologia contrattuale tipica[120], è ricondotto all'appalto di servizi considerato

---

[118] *Cfr.* A. MANTELERO, *Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, in *Dir. informazione e informatica*, 2010, p. 674 e ss.
[119] *Cfr.* D. VALENTINO, *I contratti di informatizzazione d'azienda*, in *Dir. dell'internet*, 2005, 416.
[120] Sul punto, v. E. TOSI, *Il contratto di outsourcing di sistema informatico*, Milano, 2001; A. MUSELLA, *Il contratto di outsourcing del sistema informativo*, in *Dir. informazione e informatica*, 1998, p. 857 ss.

qualificato perché diretto ad esternalizzare parte dell'attività aziendale[121] e, conseguentemente, delle risorse umane.

La tecnologia *cloud*, consentendo l'affidamento a terzi di parte di servizi informatici, è sempre più spesso utilizzata dalle imprese per porre in essere processi di *outsourcing* informatico. Da ciò scaturisce il tentativo di qualificare il contratto di *cloud* come un contratto di *outsourcing* con la conseguente applicazione della relativa disciplina. I punti di contatto tra le due fattispecie sono evidenti e possono essere sintetizzati nell'analogia di scopo costituita dall'esternalizzazione di servizi o attività. Il servizio offerto assume, in entrambi i casi, una posizione centrale da cui scaturisce l'esigenza di prevedere nel contratto, o comunque negli allegati tecnici ad esso connessi, elementi idonei a garantire e misurare la prestazione e, quindi, l'efficienza del servizio fornito anche al fine di graduare, in ragione degli stessi indicatori, i relativi costi[122].

Pur in presenza delle riferite affinità non possono essere ignorate, in sede di qualificazione del contratto di *cloud computing*, le importanti divergenze con il modello dell'*outsourcing*[123]. Deve rilevarsi, infatti, che con l'*outsourcing* non si realizza solo un'esternalizzazione delle risorse strutturali, come accade nel contratto di *cloud*, ma anche quella delle risorse umane. Il *cloud computing*, in particolar modo il cd. *public cloud*, è basato sul modello di distribuzione "uno

---

[121] V. O. CAGNASCO, G. COTTINO, *Contratti commerciali*, in *Trattato di diritto commerciale*, G. COTTINO (diretto da), Padova, 2000, p. 353; M. PITTALIS, *op. cit.*, p. 1015; A. MUSELLA, *op. cit.*, p. 859 ss.; F. CARDARELLI, *op. cit.*, p. 94.

[122] *Cfr.* N. FOGGETTI, *Privacy Protection, applicable Law and Jurisdiction Issues in Cloud Computing: an International and EU prospective*, in *Ciberspazio e dir.*, vol. 15, n. 51 (2/3-2014), p. 207 ss.

[123] V. A. MANTELERO, *Il contratto per l'erogazione alle imprese di servizi di cloud computing*, in *Contratto e impr.*, 2012, p. 1218.

a molti" per cui i contratti, standardizzati e privi di vincoli di esclusiva, sono destinati ad una pluralità di utenti.

L'*outsourcing* tradizionale, invece, è contraddistinto da un forte legame tra le parti sancito, sotto il profilo contrattuale, da clausole di esclusiva e da un'attenta personalizzazione del servizio in ragione delle esigenze del cliente.

Un'altra importante divergenza emerge dalla definizione dei costi; la standardizzazione dei contratti *cloud*, infatti, comporta un'uniformazione dei prezzi definiti sulla scorta della frequenza di utilizzo del servizio e della quantità di risorse impiegate. L'*outsourcing*, di contro, è soggetto a costi variabili in virtù della personalizzazione del servizio e delle specifiche richieste avanzate dall'*outsourcer*.

Prima di soffermarsi sulla riferibilità del contratto di *cloud computing* alla somministrazione di servizi è opportuno indagare la possibilità di qualificare lo stesso contratto di *cloud* sulla base delle norme che disciplinano la licenza d'uso[124] o la locazione.

Il nostro ordinamento non conosce un tipo negoziale denominato licenza d'uso; si tratta di un contratto atipico, utilizzato nella distribuzione del *software*[125], a cui sono ricondotti una moltitudine di accordi con specifiche peculiarità. La definizione "licenza d'uso", infatti, assicura solo apparentemente omogeneità di disciplina che, invero, è eterogenea in considerazione della moltitudine di licenze esistenti.

---

[124] *Cfr.* N. FOGGETTI, *op. cit.*, p. 210 ss.

[125] In tema di distribuzione del *software*, v. G. SISTO, *Le diverse modalità di distribuzione del software: freeware, shareware e trial version*, in G. CASSANO, *Diritto delle nuove tecnologie e dell'internet*, Milano, 2002, p. 1058 ss.

Le parti coinvolte nel contratto di licenza sono il licenziante che detiene i diritti esclusivi e cede in godimento il *software* ed il licenziatario che utilizza lo stesso *software* nel rispetto del contratto e dei limiti imposti dalla legge.

Con la cessione dei diritti di utilizzazione, come precisato, non si trasferisce la titolarità dei diritti esclusivi che restano in capo al licenziante ma, piuttosto, il diritto al godimento personale del *software*.

Il contratto di licenza d'uso del *software* cd. pacchettizzato - realizzato secondo un modello generale uguale per tutti e potenzialmente destinato a qualsiasi utente - è modellato sullo schema del contratto per adesione; le licenze d'uso sono standardizzate con l'esclusiva possibilità, per l'utente, di accettare le condizioni contrattuali determinate unilateralmente dal fornitore in assenza di qualsiasi negoziazione utile a concordare, attraverso una dichiarazione di volontà bilaterale, eventuali condizioni personalizzate.

Per un corretto inquadramento negoziale della licenza d'uso è importante valutare il relativo regolamento contrattuale e comprendere l'esatta volontà delle parti per verificare, conseguentemente, la possibilità di sussumere il contratto nelle fattispecie tipiche in ragione delle loro caratteristiche che possono avvicinarle ai diversi schemi di licenza. Alternativamente, lo stesso contratto di licenza sarà da considerare espressione della libertà contrattuale, sancita dall'art. 1322 c.c., non coincidente con le fattispecie codificate.

Con riferimento alla distribuzione del cd. *software* pacchettizzato si è tentato di ricondurre il contratto di licenza alla fattispecie della locazione sulla scorta dell'oggetto della cessione costituito dal diritto di godimento del

software[126]. Si tratterebbe in realtà di una locazione atipica[127] poiché non è possibile rinvenire un'esatta coincidenza tra la disciplina codicistica del contratto di locazione[128] e gli elementi che di fatto caratterizzano la licenza d'uso.

Se è vero, infatti, che il contratto di licenza d'uso e quello di locazione sono accomunati dalla costituzione di un diritto personale di godimento, rispettivamente sul *software* o sulla cosa locata, a fronte di un corrispettivo economico, è altrettanto vero che gli altri effetti tipici della locazione sono estranei alla quasi totalità dei modelli di distribuzione del *software* pacchettizzato[129] anche se in ogni caso, come anticipato, sarà opportuno sondare attentamente la volontà delle parti.

Si è tentato, inoltre, di ricondurre il contratto di licenza d'uso alla vendita[130] partendo dalla considerazione che la stessa è *"il contratto che ha per oggetto il trasferimento della proprietà di una cosa o il trasferimento di un altro diritto verso il corrispettivo di un prezzo"*. L'ampiezza della definizione ed in particolare il riferimento al trasferimento della proprietà di un altro diritto, al

---

[126] Sul punto, v. F. GALGANO, *La cultura giuridica italiana di fronte ai problemi informatici*, in G. ALPA, V. ZENO ZENCOVICH, *I contratti d'informatica*, Milano, 1986, p. 379; S. LEONE, *La concessione del software tra licenza e locazione*, in G. ALPA, V. ZENO ZENCOVICH, *I contratti d'informatica*, Milano, 1986, p. 349; G. FINOCCHIARO, *I contratti ad oggetto informatico*, Padova, 1993, p. 94.

[127] V. C. ROSSELLO, *I contratti dell'informatica nella nuova disciplina del software*, Milano, 1997, p. 66; E. BONAZZI, C. TRIBERTI, *Guida ai contratti dell'informatica*, Milano, 1990, p. 57.

[128] *Cfr.* artt. 1571 ss., c.c.

[129] Si pensi, ad esempio, alle modalità di pagamento del corrispettivo che solitamente viene versato in un'unica soluzione e non periodicamente o ancora alla durata del rapporto che non ha i limiti previsti dall'art. 1573 c.c. Il licenziatario, inoltre, non risponde, nei confronti del licenziante, della perdita o del deterioramento del bene ma, piuttosto, ne assumerà personalmente il rischio. In argomento *cfr.* M. FARINA, *Creazione e distribuzione di proprietà intellettuale*, in *I contratti dell'informatica, Aspetti civilistici e fiscali*, A. ATTANASIO, G. BELLAZZI, D. D'AGOSTINI, M. FARINA, Forlì, 2008, p. 67.

[130] M. BIN, *L'equilibrio sinallagmatico nei contratti informatici*, in G. ALPA, V. ZENO ZENCOVICH, *I contratti d'informatica*, Milano, 1986, p. 65.

pagamento di un prezzo *una tantum* ed alla durata indeterminata del trasferimento, hanno fatto pensare all'associazione del contratto di licenza a quello di vendita. Non può trascurarsi, però, che nella quasi totalità delle licenze sono presenti clausole contrattuali che prevedono una cessione del diritto di utilizzo del *software*, riservando al titolare del diritto di esclusiva lo sfruttamento economico dell'opera e, quindi, il potere di controllo sulla sua circolazione. Tali clausole sono assolutamente incompatibili con il principio di esaurimento previsto dall'art. 64 *bis*, lett. c), l. 633/41 e, conseguentemente, con lo schema della compravendita. La citata disposizione, infatti, prevede espressamente che *"[...] La prima vendita di una copia del programma nella Comunità Economica Europea da parte del titolare dei diritti, o con il suo consenso, esaurisce il diritto di distribuzione di detta copia all'interno della Comunità, ad eccezione del diritto di controllare l'ulteriore locazione del programma o di una copia dello stesso"*; l'utilizzo di un contratto di compravendita, pertanto, avrebbe l'evidente effetto di privare il venditore di ogni diritto esclusivo di distribuzione sul prodotto *software*.

Si avrà, in ogni caso, esaurimento del diritto esclusivo di distribuzione della copia di un *software* quando il titolare del diritto autorizza l'utente, a fronte di una remunerazione *"corrispondente al valore economico della copia dell'opera di cui è proprietario"*, ad utilizzare il *software* stesso senza limitazioni di durata. Conseguentemente, in caso di cessione a terzi della licenza di utilizzazione concessa senza limitazioni di durata, il nuovo utilizzatore, avvalendosi dell'esaurimento del diritto di distribuzione, potrà essere considerato legittimo titolare della copia del *software* e potrà utilizzarla

purché il suo *dante causa* renda inutilizzabile la propria copia al momento della cessione[131].

Ancora una volta è chiara l'importanza di indagare la volontà delle parti prescindendo dal *nomen iuris* utilizzato per individuare il modello negoziale tipico di riferimento inquadrando, in alternativa, il contratto di licenza d'uso come un contratto misto o atipico in senso stretto.

Dall'analisi effettuata emerge che il contratto di licenza d'uso, pur caratterizzato per una flessibilità che ben si sposerebbe con la qualificazione giuridica del contratto di *cloud computing*, non è in grado di ricomprendere interamente le molteplici tipologie di *cloud computing*. Si potrebbe adattare, al più, ai servizi SaaS non trovando spazio, invece, per le attività di memorizzazione dei dati o per l'erogazione degli altri servizi complessi precedentemente descritti.

Non è mancato il tentativo di qualificare il contratto di *cloud computing* direttamente sulla base del contratto di locazione prescindendo dal riferimento alla licenza d'uso.

Come è noto con il contratto di locazione *"[...] una parte si obbliga a far godere all'altra una cosa mobile o immobile per un dato tempo, verso un determinato corrispettivo"*; la possibilità per l'utente di archiviare dati su *hardware* messo a disposizione, gestito e manutenuto, da un *cloud provider*

[131] V. Corte giust., 3 luglio 2012, C-128/11, Caso Used Soft GmbH c. Oracle International Corp, in *http://curia.europa.eu/juris/document/document.jsf?docid=124564&doclang=IT*.

costituirebbe espressione della possibilità del far godere una cosa per un certo periodo di tempo[132].

Si tratterebbe di una soluzione adattabile alla fornitura di servizi IaaS e PaaS. Per i servizi SaaS, invece, in considerazione delle loro specifiche caratteristiche, si potrebbe al più optare per la disciplina della locazione contaminata da caratteristiche proprie del contratto di licenza d'uso; si parlerà, in tal caso, ancora una volta, di un contratto misto.

3.1.- *(Segue) Il contratto di cloud computing come somministrazione di servizi.*

Il modello contrattuale a cui sembra aderire meglio il contratto di *cloud computing* è quello della somministrazione di servizi considerata oggi - a seguito dell'evoluzione dell'orientamento dottrinale tradizionale che limitava il concetto di somministrazione all'esecuzione di una prestazione, periodica e continuativa, di cose[133] - disciplina di riferimento dei contratti aventi ad oggetto prestazioni continuative o periodiche di servizi.

Il contratto di *cloud computing*, sotto un profilo di classificazione giuridica, può essere ricondotto tra i contratti di durata aventi ad oggetto servizi automatizzati o meccanizzati e, più precisamente, tra quelli aventi ad oggetto

---

[132] Sulla possibilità di applicare la disciplina della locazione anche all'ipotesi di utilizzo del *software* v. Direttiva 2009/24/CE del Parlamento europeo e del Consiglio, relativa alla tutela giuridica dei programmi per elaboratore, che, al considerando n. 12, ha statuito che *"[...] per 'locazione' s'intende il mettere a disposizione per l'utilizzazione, per un periodo limitato e per fini di lucro, un programma per elaboratore o una copia dello stesso; tale termine non comprende il prestito pubblico, che esula pertanto dagli obiettivi della presente direttiva"*.

[133] Per una completa ricostruzione dell'evoluzione del contratto di somministrazione l'autorevole contributo di R. BOCCHINI, *Il contratto di somministrazione di servizi*, in *I contratti di somministrazione e di distribuzione*, R. BOCCHINI, A. GAMBINO, Torino, 2011, p. 5 ss.

servizi informatici in senso stretto. Tale tipo di classificazione, che differisce rispetto a quella dei contratti di durata aventi ad oggetto servizi offerti dall'uomo, determina l'applicazione di una disciplina differente come accade, ad esempio, con riferimento al profilo della responsabilità nell'ambito dei contratti aventi ad oggetto servizi automatizzati; in tal caso, infatti, per l'adempimento dell'obbligazione è sufficiente la messa a disposizione, da parte del fornitore del servizio, di prodotti funzionanti ed adeguatamente manutenuti, idonei a garantire la fruizione di quanto contrattualizzato[134].

L'opportunità di ricondurre il contratto di *cloud computing* alle norme in materia di somministrazione[135], scaturisce da una ricostruzione che consente di superare l'orientamento basato sull'applicazione della disciplina in materia di somministrazione alle sole ipotesi di contratti aventi ad oggetto prestazione di cose. Tale obiettivo può essere raggiunto partendo dalla lettura congiunta degli artt. 1677 e 1570 c.c.; in particolare, l'art. 1677 c.c. – prevedendo che *"se l'appalto ha per oggetto prestazioni continuative o periodiche di servizi, si osservano, in quanto compatibili, le norme di questo capo e quelle relative al contratto di somministrazione"* – non reca alcuna selezione tra le due

[134] Per una più ampia descrizione della diversa disciplina da applicare, rispettivamente, ai contratti aventi ad oggetto servizi automatizzati e a quelli aventi ad oggetto prestazioni personali v. R. BOCCHINI, *op. cit.*, p. 8 ss.

[135] In dottrina, sulla riconducibilità del contratto di *cloud computing* alla somministrazione di servizi partendo dalla differente natura dell'obbligazione cui una delle parti, rispettivamente l'appaltatore o il somministrante, si obbliga v. D. MULA, *Il contratto di archiviazione e gestione da remoto dei documenti informatici. Qualificazione del contratto di cloud service*, in *Ianus*, 2014, n. 2. L'autore, in particolare, precisa che *"nell'appalto si rinviene un'obbligazione di fare che l'appaltatore si obbliga ad eseguire in un dato termine, più o meno lungo, al fine di soddisfare un bisogno immediato del committente. La somministrazione, invece, si caratterizza per la soddisfazione di un bisogno duraturo attraverso l'adempimento di un'obbligazione di dare a titolo definitivo o in godimento"* arrivando poi alla conclusione che, l'attività del *cloud provider* non *"[…] pare potersi certo inquadrare tra le obbligazioni di fare, giacché non è diretta alla produzione di una res nova, ma pare invero debba essere annoverata tra le prestazioni di far godere"*.

discipline richiamate mentre l'art. 1570 c.c. – statuendo che *"si applicano alla somministrazione in quanto compatibili con le disposizioni che precedono, anche le regole che disciplinano il contratto a cui corrispondono le singole prestazioni"* – fissa un criterio di gerarchia a favore delle norme sulla somministrazione.

Le due norme, quindi, avendo diverso contenuto, non sono tra loro corrispondenti e, pertanto, al contratto di *cloud* potranno applicarsi, in prima battuta, le disposizioni sulla somministrazione e, successivamente, quelle in materia di appalto – o, comunque, quelle relative ad altro schema tipico in cui è, eventualmente, sussunta la fattispecie del *cloud* – compatibili con le stesse norme sulla somministrazione[136].

È evidente, alla luce di quanto sopra, che l'art. 1677 c.c. dichiara, di fatto, applicabili le norme in materia di somministrazione al contratto avente ad oggetto la prestazione di servizi di durata; inoltre, dal richiamo implicito all'art. 1570 c.c., effettuato dallo stesso art. 1677 c.c., scaturisce la sicura attuazione del criterio di prevalenza ivi previsto[137].

---

[136] Si consideri, ad esempio, l'orientamento che qualifica il servizio IaaS come deposito irregolare (E. PROSPERETTI, *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema cloud*, in *Trattato di Diritto dell'Internet*, G. CASSANO (a cura di), Padova, 2012, p. 683). In tal caso, il quadro normativo di riferimento si dovrebbe basare sulle norme in tema di somministrazione e su quelle in tema di deposito.

[137] Sull'originaria previsione, nei lavori preparatori del codice, di una disciplina in tema di somministrazione basata sulla prestazione continuativa sia di "cose" che di "servizi" v. R. BOCCHINI, *op. cit.*, p. 19 che, tra l'altro, evidenzia come *"la ricerca più recente ha, altresì, evidenziato che la mutilazione, all'ultimo momento, dell'espressione "servizi", nella definizione dell'art. 1559 c.c., non trova, nei lavori preparatori, giustificazione alcuna, e, quel che più conta, lascia del tutto inalterate le singole norme sulla somministrazione che pensate originariamente con riferimento sia alle cose, sia ai servizi, rimangono bivalenti nel testo definitivo del codice e, cioè, perfettamente applicabili in massima parte sia ai contratti aventi ad oggetto la prestazione di cose, sia ai contratti aventi ad oggetto la prestazione di servizi"*.

Come evidenziato dalla dottrina[138], l'art. 1570 c.c., in virtù del principio *lex specialis derogat generali*, prevale sulla disciplina dell'appalto poiché le norme sulla somministrazione, pensate in ragione della durata della prestazione, devono essere considerate principali e prevalenti rispetto a quelle regolanti l'appalto che, invece, sono dirette alle prestazioni istantanee.

Ricondotto il contratto di *cloud computing* alla fattispecie tipica della somministrazione è opportuna una panoramica delle disposizioni applicabili con riferimento agli elementi costitutivi del contratto, alla sua esecuzione e, infine, alla sua estinzione.

L'art. 1560 c.c., relativo all'entità della somministrazione, consente la stipula di un contratto di somministrazione anche nelle ipotesi in cui il suo oggetto non è determinato e non è determinabile. Il rapporto negoziale, infatti, è teso a soddisfare bisogni duraturi, variabili per natura e non prevedibili al momento della conclusione dell'accordo. Negli altri tipi contrattuali, invece, com'è noto, la determinazione o la determinabilità dell'oggetto è requisito di validità del contratto.

Ai sensi della previsione codicistica, ove non è determinata l'entità della somministrazione, la stessa verrà erogata secondo il normale fabbisogno determinabile sulla base di criteri oggettivi[139]. L'ampio margine di autonomia

---

[138] *Cfr.* R. BOCCHINI, *op. cit.*, p. 19.

[139] Sulla necessità di parametrare il normale fabbisogno alle necessità normali e effettive del somministrato senza che l'erogazione possa divenire abnorme a seguito della conclusione del contratto, v. G. ZUDDAS, *Somministrazione. Concessione di vendita. Franchising, in Trattato di diritto commerciale*, V. BUONOCORE (diretto da), Torino, 2003, p. 36; G. COTTINO, *Del contratto estimatorio. Della somministrazione*, in *Commentario del codice civile*, A. SCIALOJA, G. BRANCA (a cura di), Bologna, 1970, p. 128. In argomento v. anche Trib. Pavia 22.02.86, in *Giur. merito*, 1987, p. 621 secondo cui *"la valutazione del normale fabbisogno del somministrato non è rimessa all'arbitrio del creditore, ma deve risultare da un ragionevole e diligente giudizio di prevedibilità"*.

di cui godono le parti contrattuali nella definizione e nella quantificazione del servizio da erogare è solitamente ricondotto allo schema del *pay for use* e delle tariffe *flat*.

Nel primo caso l'utente è completamente libero di scegliere caratteristiche, quantità e qualità delle risorse *hardware* e *software* da impiegare pagando il prezzo dovuto in ragione delle sue opzioni; nel secondo caso, invece, a fronte del pagamento di un canone fisso è prevista l'erogazione di una quantità minima di risorse dalle caratteristiche predefinite fatta salva la possibilità per l'utente di chiedere un'estensione dell'offerta con accesso ad ulteriori servizi anche sotto il profilo qualitativo[140].

Con riferimento alla determinazione del prezzo, invece, non può trovare applicazione l'art. 1561 c.c.[141] poiché lo stesso ha ad oggetto la determinazione del prezzo nella sola somministrazione periodica di servizi e non anche nella somministrazione a carattere continuativo in cui non è possibile ipotizzare la scadenza delle singole prestazioni. Il riferimento, deve essere, allora, al disposto dell'art. 1657 c.c. che – in caso di omessa determinazione del corrispettivo o della mancata indicazione della modalità per determinarlo – rinvia, alternativamente, alle tariffe, agli usi o alla determinazione del Giudice.

Il divieto di subappalto previsto dall'art. 1656 c.c., pur non ponendosi in contrasto con le norme sulla somministrazione, non trova applicazione

---

[140] In merito alla maggiore idoneità di questo modello a contemperare gli opposti interessi delle parti, v. R. BOCCHINI, *Sub art. 1560 c.c.*, in *Dei singoli contratti. Artt. 1548-1654*, D. VALENTINO (a cura di), in *Commentario del Codice civile*, GABRIELLI (diretto da), Torino, 2011, p. 192.

[141] Art. 1561 c.c. *"Nella somministrazione a carattere periodico, se il prezzo deve essere determinato secondo le norme dell'art. 1474, si ha riguardo al tempo della scadenza delle singole prestazioni e al luogo in cui queste devono essere eseguite"*.

nell'ipotesi di servizi erogati in modo automatizzato poiché in tali circostanze viene a mancare l'elemento fiduciario caratterizzante il contratto di appalto e posto alla base della *ratio* dello stesso divieto.

Il contratto di *cloud computing*, però, a differenza delle altre ipotesi di servizi automatizzati, si caratterizza per l'importanza dell'elemento fiduciario; l'affidabilità del *cloud provider* ed il possesso da parte di quest'ultimo di idonee certificazioni relative alla organizzazione aziendale ed alla gestione della sicurezza delle informazioni trattate, sono sicuramente elementi determinanti per la scelta dell'utente e la conclusione del contratto.

Attesa la rilevanza dell'elemento fiduciario – da intendere come aspettativa a che solo il *provider* scelto fornisca, con regolarità, i servizi individuati nel rispetto delle modalità concordate – si deve ritenere applicabile, anche al contratto di *cloud computing*, il divieto di subappalto previsto dall'art. 1656 c.c.

In fase esecutiva, possono regolare il contratto di *cloud computing* le previsioni di cui agli artt. 1562, 1563, 1564 e 1662, co. 1, c.c.

L'art. 1562 c.c.[142] disciplina il pagamento del prezzo che, nel caso in esame, trattandosi di somministrazione a carattere continuativo è da corrispondere secondo le scadenze d'uso solitamente bimestrali o mensili.

L'eventuale mancata previsione contrattuale determina, ai sensi dell'art. 1347 c.c., un'automatica applicazione della predetta norma[143] con possibilità per le parti di definire le specifiche modalità di pagamento.

---

[142] L'art. 1562 c.c. così dispone: *"1. Nella somministrazione a carattere periodico il prezzo è corrisposto all'atto delle singole prestazioni e in proporzione di ciascuna di esse.*
2. Nella somministrazione a carattere continuativo il prezzo è pagato secondo le scadenze di uso".

La previsione di cui all'art. 1563 c.c. può essere considerata, limitatamente a quanto disposto dal primo comma, per il termine iniziale; nel contratto di *cloud computing* a carattere continuativo, infatti, non ha rilevanza il riferimento al termine finale che ha il compito di indicare il periodo massimo in cui le parti si obbligano alle reciproche prestazioni[144].

Può ritenersi applicabile al *contratto cloud* il disposto dell'art. 1662 c.c. integrato con le previsioni dell'art. 1564 c.c. In particolare, l'utente *cloud* ha diritto di controllare *"lo svolgimento dei lavori"* avendo come parametro di riferimento i livelli quantitativi e qualitativi contrattualmente fissati con la possibilità - nel caso di un inadempimento di notevole importanza *"tale da menomare la fiducia nell'esattezza dei successivi adempimenti"* - di richiedere la risoluzione dello stesso contratto.

La disciplina in materia di appalto prevede specifiche disposizioni in merito all'eventuale esigenza di apportare delle variazioni a quanto originariamente concordato. Si può ipotizzare che, anche nel contratto di *cloud*, in ragione della sua durata continuata, ci si debba confrontare con tale esigenza.

Il riferimento normativo è da ricercare, nei termini di seguito meglio specificati, negli artt. 1659, 1660 e 1661 c.c.; le variazioni possono essere relative alla quantità ma anche alla qualità ed alla tipologia del servizio offerto[145]. L'utente potrà optare, ove rilasciata e disponibile, per una nuova

---

[143] Sul punto, *cfr.* Cass. 29 settembre 2004 n. 19531, in *Rep. Foro it*., *2004,* voce *Contratto in genere [1740]*, n. 468.

[144] *Cfr.* R. BOCCHINI, *Sub art. 1563 c.c.*, in *Dei singoli contratti, Artt. 1548-1654*, D. VALENTINO (a cura di), in *Commentario del Codice Civile*, GABRIELLI, (diretto da), Torino, 2011, p. 221.

[145] Sul tema della variazione in materia di servizi, v. M. RUBINO SAMMARTANO, *Appalti di opere e contratti di servizi (in diritto privato)*, Padova, 2006, p. 734.

versione del servizio offerto, fermo restando che, in caso di minime modifiche, non gli potranno essere addebitati costi ulteriori.

In tema di variazioni concordate è possibile considerare l'art. 1659 c.c. sia pur limitatamente ai primi due commi che vietano la variazione unilaterale del contenuto del contratto. Quanto al terzo comma, invece, è da evidenziare la sua inapplicabilità poiché, in un contratto di somministrazione, la fruizione di una prestazione in misura eccedente quella determinata, obbliga l'utente somministrato a pagare l'intero[146].

Gli artt. 1660 e 1661 c.c. che regolano, rispettivamente, le variazioni necessarie ai fini dell'esecuzione del contratto e quelle richieste dal somministrato con conseguente diritto per il somministrante di ottenere un incremento del corrispettivo dovuto, possono essere applicati al contratto di *cloud computing*.

Il riferimento in materia di eccessiva onerosità sopravvenuta dovrà essere l'art. 1467 c.c. attesa l'inutilizzabilità dell'art. 1664 c.c. espressamente riferito all'appalto d'opera[147].

Relativamente alla fase di esecuzione del contratto di *cloud computing* potranno anche essere presi in considerazione, in ragione della stessa struttura contrattuale che deve caratterizzarsi per la chiara indicazione delle modalità di erogazione dei servizi, gli artt. 1667 e 1668 c.c. recanti previsioni in tema di garanzia per vizi e difformità della prestazione. Il *provider* somministrante, infatti, deve fornire un servizio conforme a quanto convenuto e, ove ciò non

[146] V. sul punto R. BOCCHINI, *op. cit.*, p. 24.
[147] *Cfr.* M. RUBINO SAMMARTANO, *op. cit.*, p. 734.

accada, l'utente somministrato dovrà denunciare la difformità o il vizio entro sessanta giorni dalla sua scoperta sempre se la difformità o il vizio non erano da lui conosciuti o riconoscibili al momento dell'accettazione del servizio. La garanzia prevista dall'art. 1667 c.c. consta nella possibilità per il somministrato di chiedere l'eliminazione, a spese del somministrante, di difformità o vizi ovvero la riduzione proporzionale del prezzo fatta salvo, in caso di colpa dello stesso somministrante, il diritto al risarcimento del danno. L'utente per ottenere la garanzia *de qua* avrà l'onere di denunciare il vizio e di provarne la tempestività a differenza di quanto accadrà nel caso in cui intende far valere l'ordinaria responsabilità contrattuale.

I diritti scaturenti dal contratto di *cloud computing* potranno essere fatti valere nel termine ordinario di dieci anni[148] poiché la prescrizione breve di due anni, prevista in materia di appalto dal terzo comma dell'art. 1667 c.c., è una norma eccezionale la cui *ratio*, ispirata alla consegna dell'opera ed alla natura circoscritta nel tempo dello stesso contratto di appalto, non ricorre nel contratto di somministrazione che, nel caso in esame, si caratterizza per una prestazione continuativa di servizi[149].

L'inadempimento di lieve entità da parte dell'utente somministrato, ai sensi dell'art. 1565 c.c., non può comportare la sospensione dell'esecuzione del contratto fatta salva l'esistenza di un congruo preavviso in tal senso da parte del somministrante. Si potrà procedere, invece, alla sospensione immediata

[148] È opportuno ricordare, in ogni caso, che ai sensi dell'art. 2948, n. 4, c.c., si prescrivono in cinque anni *"gli interessi e in generale, tutto ciò che deve pagarsi periodicamente ad anno o in termini più brevi"*.
[149] *Cfr.* R. BOCCHINI, *op. cit.*, p. 25.

della prestazione, *ex* art. 1460 c.c., in tutti i casi in cui l'inadempimento non è di lieve entità.

In presenza di un contratto di somministrazione a tempo indeterminato, quale può essere considerato il contratto di *cloud*, ciascuna parte, ai sensi dell'art. 1569 c.c., può recedere, senza obbligo di corrispettivo, dandone preavviso nel termine pattuito o in quello stabilito dagli usi o, in mancanza, in un termine congruo in ragione della natura della prestazione.

Il preavviso, secondo parte della dottrina[150], non necessita di una particolare forma. Anche in sua assenza, il recesso sarà valido fatto salvo il diritto, per la parte che lo subisce, di ottenere il risarcimento del danno.

Non manca però chi[151], in modo convincente, ritiene il preavviso *ex* art. 1569 c.c. presupposto del recesso e condizione di efficacia dello stesso. Il citato articolo, infatti, a differenza di quanto previsto dall'art. 2118 c.c., non prevede alcuna indennità sostitutiva del preavviso da cui poter far discendere una diversa conclusione.

È applicabile al contratto di *cloud computing* anche la previsione di cui all'art. 1564 c.c. che regola la risoluzione del contratto nel caso di un inadempimento di non notevole importanza *"tale da menomare la fiducia nell'esattezza dei successivi adempimenti"*.

La disposizione opera a vantaggio tanto del somministrante quanto del somministrato; la valutazione della *"notevole importanza"* dell'inadempimento deve essere effettuata utilizzando, come parametro di riferimento, il

---

[150] V. C. GIANNATTASIO, *L'appalto*, *op. cit.*, p. 227; G. COTTINO, *Del contratto estimatorio. Della somministrazione*, *op. cit.*, p. 201.
[151] V. R. BOCCHINI, *Sub art. 1569 c.c.*, in *Dei singoli contratti. Artt. 1548-1654*, *op. cit.*, p. 263.

regolamento contrattuale al fine di rilevare il reale pregiudizio subito da una delle parti che, a causa della condotta del soggetto inadempiente, vede frustrate le sue legittime aspettative. La lesione della fiducia nei successivi adempimenti, poi, non può essere valutata arbitrariamente ma, piuttosto, deve essere una chiara conseguenza dello stesso inadempimento[152].

4.- *Il contratto di cloud computing come contratto misto.*

Pur ritenendo la somministrazione il modello a cui meglio si adatta il contratto di *cloud computing* è indubbio che lo stesso modello potrà essere considerato riferimento prevalente ma non esclusivo.

L'interprete, infatti, dopo aver determinato il diritto applicabile al contratto sulla scorta dei meccanismi descritti in precedenza[153], deve indagare la concreta volontà delle parti e, quindi, l'obiettivo del negozio assicurando la miglior tutela degli interessi coinvolti per il tramite di un'interpretazione sistematica che consenta l'individuazione e l'utilizzo della disciplina più idonea tra le diverse soluzioni adottabili.

Pertanto – in assenza di uno specifico intervento normativo che tenga conto della complessa articolazione della tecnologia *cloud* definendo, in modo preciso, gli obblighi che le parti contrattuali assumono nella fornitura di servizi *cloud* – sarà possibile riferirsi al modello, anche atipico, più rispondente alle esigenze del singolo caso concreto.

---

[152] In argomento, *cfr.* R. BOCCHINI, *Sub art. 1564 c.c.*, in *Dei singoli contratti. Artt. 1548-1654*, *op. cit.*, p. 263.
[153] V. il precedente capitolo 2.

Il contratto di *cloud computing*, come già rilevato, si inserirà spesso in un complesso di operazioni negoziali recanti un'autonoma disciplina con la conseguente necessità di delimitare i relativi confini di operatività. In tal caso, ci si deve confrontare con un contratto misto in cui, per l'appunto, confluiscono la causa e la disciplina di più figure contrattuali diverse con la conseguente commistione di istituti diversi in un nuovo contratto – con un'unica causa concreta alla base della valutazione di meritevolezza e di liceità dello stesso contratto – finalizzato al perseguimento di un risultato unitario.

La disciplina complessiva del contratto misto è il risultato della combinazione delle specifiche disposizioni rispondenti alle diverse componenti negoziali confluite nel regolamento unitario adottato dalle parti.

La teoria della combinazione, infatti, comporta che a ciascun tipo negoziale coinvolto, previo un opportuno coordinamento, sia applicata la normativa che gli è propria se compatibile con la specifica fattispecie[154].

Nell'ipotesi in cui il contratto misto è particolarmente influenzato dagli elementi di un determinato tipo contrattuale, la disciplina del contratto prevalente prevarrà su quella del contratto non prevalente che, comunque, potrà essere applicata nei limiti della sua compatibilità con la prima[155].

---

[154] Sul punto, v. M. BIN, *L'equilibrio sinallagmatico nei contratti informatici*, in AA.VV., *I contratti di informatica: profili civilistici, tributari e di bilancio*, a cura di G. ALPA – V. ZENO ZENCOVICH, VII, Milano, 1987, p. 68 ss.; F. BOCCHINI, E. QUADRI, *Diritto Privato*, V edizione, Torino, 2014, p. 848 ss.

[155] *Cfr.* Cass. 20 gennaio 2005, n. 1150, secondo cui *"[…] in tema di contratto misto, il negozio deve essere assoggettato alla disciplina unitaria dell'uno o dell'altro contratto in base alla prevalenza degli elementi, salva l'applicazione degli elementi del contratto non prevalente se regolati da norme compatibili con quelle del contratto prevalente"*.

Tale soluzione risponde al più recente orientamento giurisprudenziale teso ad unificare il criterio dell'assorbimento con quello della combinazione[156].

In particolare, la giurisprudenza ha adottato il riferito correttivo rendendosi conto che dall'utilizzo esclusivo del criterio dell'assorbimento – da lei tradizionalmente seguito e basato sull'applicazione, al contratto misto, della sola disciplina normativa del tipo contrattuale prevalente – deriva il serio rischio di trascurare la reale volontà delle parti che potrebbero non vedere tutelati gli interessi in concreto perseguiti[157].

5.- *Il cloud computing e la standardizzazione delle clausole contrattuali.*

Alla luce di quanto sino ad ora illustrato è evidente che il contratto costituisce lo strumento fondamentale per regolare le modalità con cui devono essere erogati i servizi *cloud*.

In quest'ottica non può omettersi un riferimento alle azioni poste in essere dalla Commissione Europea nell'ambito della strategia tesa a sfruttare pienamente le potenzialità del *cloud computing* in Europa.

Come già rilevato, la Commissione ha sottolineato[158] l'importanza di interventi mirati per accrescere la fiducia nelle soluzioni di *cloud* garantendo l'interoperabilità tecnica delle piattaforme, la portabilità dei dati e

---

[156] Deve rilevarsi l'esistenza di una terza teoria, cd. dell'analogia, secondo cui il contratto misto sarebbe un contratto innominato soggetto, quindi, all'applicazione analogica del contratto tipico più simile.

[157] In argomento, v. F. CARINGELLA, L. BUFFONI, *Manuale di diritto civile*, VI edizione, Roma, 2016, p. 757 ss.

[158] V. Comunicazione della Commissione Europea al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Sfruttare il potenziale del cloud computing in Europa*, 27.09.12, COM(2012) 529 final, reperibile su *http://ec.europa.eu/transparency/regdoc/rep/1/2012/IT/1-2012-529-IT-F1-1.Pdf*.

l'interoperabilità giuridica dei contratti alla base dei servizi *cloud* con l'obiettivo della definizione di uno *standard* contrattuale.

In quest'ottica, nel febbraio 2013, è stato istituito un gruppo di lavoro, composto da *stakeholder*, a cui è stato affidato il compito di individuare *clausole* per la standardizzazione dei livelli di servizio *cloud* nei contratti di fornitura tra i "*cloud providers*" e i "*cloud service customers*"; tale esigenza è scaturita, in particolar modo, dall'estensione del fenomeno *cloud* e dal frequente coinvolgimento nei rapporti negoziali di soggetti appartenenti a giurisdizioni diverse.

L'attività del gruppo di lavoro è confluita nelle "*Cloud Service Level Agreement Standardisation Guidelines*"[159] con cui sono stati definiti, in modo sistematico, i livelli di servizio *cloud* indicandone da un lato, i fattori di criticità e, dall'altro, i criteri e i parametri di funzionalità tramite la descrizione di vari indicatori quali la disponibilità, l'affidabilità e la qualità dei servizi forniti nonché i livelli di sicurezza e protezione dei dati immessi nel *cloud*.

Le linee guida, inoltre, con la standardizzazione dei sistemi tecnologici e di sicurezza, hanno puntato a rafforzare i diritti degli utenti garantendo la riservatezza delle informazioni e la possibilità di controllare e gestire in qualsiasi momento i propri dati.

Particolare attenzione è stata dedicata alle condizioni contenute nel *Service Level Agreement* (SLA) che, come già precisato, costituisce una componente fondamentale del contratto di *cloud computing*.

---

[159] Pubblicate nel giugno 2014 e reperibili su *https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines*.

Il gruppo di lavoro non si è limitato ad offrire definizioni tecniche da condividere e richiamare nei vari contratti ma si è anche concentrato sulla valutazione dei livelli di servizio che costituiscono parametro fondamentale per verificare l'esatto adempimento contrattuale del *cloud provider*. Invero, non è stato previsto quale livello può essere considerato accettabile ma, piuttosto, sono state indicate le clausole che è opportuno inserire nei contratti[160].

Le linee guida, così strutturate, hanno permesso di raggiungere il duplice obiettivo di orientare, da un lato, i *cloud provider* nella redazione delle condizioni contrattuali e di consentire, dall'altro, agli utenti, una scelta consapevole nel vasto panorama delle offerte *cloud*. Questi ultimi, infatti, utilizzando le *guidelines* come parametro di riferimento, potranno comparare servizi e condizioni dei diversi *provider* valutando la completezza dell'offerta senza poter contare, però, su indicazioni in merito alla qualità degli stessi servizi.

La Commissione, forse, avrebbe potuto utilizzare uno strumento più incisivo rispetto alle linee guida che, di fatto, non hanno una portata vincolante e costituiscono un mero parametro di riferimento da cui è possibile anche discostarsi. Una presa di posizione sui livelli qualitativi minimi delle prestazioni, inoltre, avrebbe consentito all'utente di valutare meglio la rispondenza alle proprie esigenze del servizio proposto.

È opportuno rilevare, infine, che l'ambito di applicazione delle linee guida è stato circoscritto ai *"cloud services customers (not being consumers)"*;

[160] Si pensi, a titolo esemplificativo, alle clausole relative alla modalità in cui è fornita l'assistenza tecnica con l'indicazione della relativa tempistica.

sembrerebbe, quindi, in altre parole, che i principi delle *guidelines* non sono da applicare ai contratti con i consumatori. Invero, considerando la natura dello strumento utilizzato, si ritiene che non esiste alcuna causa ostativa all'estensione dei predetti principi anche ai consumatori; tal conclusione è altresì suffragata dalla considerazione che i servizi *cloud* sono servizi della società dell'informazione previsti dalla Direttiva 2000/31/CE che non fa alcun riferimento alla nozione di consumatore riferendosi, invece, semplicemente all'utente. Ciò accade perché la Direttiva focalizza l'attenzione sulla particolare natura del servizio offerto ponendo sullo stesso piano professionisti e consumatori. Il d.lgs. 70/03, inoltre, recependo la citata Direttiva, ha ampliato l'applicazione delle previsioni a tutela del consumatore alle ipotesi in cui il rapporto tra il fornitore dei servizi e l'utente avviene in assenza di un canale di comunicazione individuale come accade, ad esempio, nel caso di contratti conclusi con la modalità del *point and click*[161].

La Commissione Europea, nell'ottobre del 2013, per incrementare la fiducia dei consumatori nell'utilizzo di servizi di *cloud computing*, ha anche istituito un gruppo di esperti conferendo l'incarico di individuare clausole contrattuali sicure ed eque, ferma restando la facoltatività del loro impiego.

[161] Sul punto, v. D. MULA, *Standardizzazione delle clausole contrattuali di somministrazione di servizi cloud e benessere del consumatore*, in *Profili interdisciplinari del commercio elettronico*, C. G. CORVESE, G. GIMIGLIANO (a cura di), Pisa, 2016, p. 146. In generale, sul tema della tutela del consumatore telematico v., *ex multis*, R. CLARIZIA, *Contratti e commercio elettronico*, in *Manuale di informatica giuridica e diritto delle nuove tecnologie*, M. DURANTE, U. PAGALLO, Torino, 2012, p. 316 ss.; E. MINERVINI, P. BARTOLOMUCCI, *La tutela del consumatore telematico*, in *Manuale di Diritto dell'informatica*, D. VALENTINO (a cura di), Napoli, 2016, p. 347.

Il lavoro degli esperti ha prodotto il *report "Comparative study on cloud computing contracts"*[162] e si è concentrato, in un'ottica comparatistica, sull'analisi di questioni relative alla qualità dei servizi *cloud*, alla possibilità di effettuare modifiche contrattuali in costanza del rapporto ed, infine, alle ipotesi di responsabilità contrattuale.

Tale attività è risultata determinante, insieme a tante altre poste in essere, per consentire alla Commissione Europea di giungere alla presentazione della proposta di direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale[163] categoria, questa, in cui possono essere inseriti a pieno titolo i servizi di *cloud computing*.

La proposta è stata presentata nell'ambito della Strategia per il mercato unico digitale[164] tesa allo sviluppo di un'economia digitale idonea, attraverso il superamento della frammentazione del quadro normativo esistente, a creare nuova occupazione con l'espansione dei mercati[165].

L'obiettivo della proposta di direttiva è quello di superare, grazie all'armonizzazione normativa, l'incertezza legata alla diversità e complessità

---

[162] Pubblicato nel marzo 2015 e reperibile su *http://bookshop.europa.eu/en/comparative-study-on-cloud-computing-contracts-pbDS0115164/*.

[163] V. Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*, reperibile su *http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52015PC0634&from=it*. Invero la Commissione – nell'ambito della Strategia per il mercato unico digitale – ha presentato, contestualmente alla prima, in occasione della Comunicazione *"Contratti nel settore digitale per l'Europa - Sfruttare al massimo il potenziale del commercio elettronico"*, una seconda proposta di direttiva relativa a determinati aspetti dei contratti di vendita *online* e di altri tipi di vendita a distanza di beni, 09.12.15, COM(2015) 635 *final*, reperibile su *https://ec.europa.eu/transparency/regdoc/rep /1/2015/IT/1-2015 -635-IT-F1-1.PDF*.

[164] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Strategia per il mercato unico digitale in Europa, 06.05.15, COM(2015) 192 *final*, reperibile su *http://eurlex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52015DC0192&from=IT*.

[165] Il mercato unico digitale, secondo stime della Commissione Europea, potrebbe determinare un aumento del PIL dell'UE di circa 415 miliardi di euro con nuove opportunità sia per le imprese già operative sul mercato che per le *start up*.

del quadro giuridico di riferimento a causa delle differenze tra i singoli diritti nazionali che costituiscono i principali ostacoli allo sviluppo dell'offerta di contenuti digitali.

La proposta, insieme a quella relativa a determinati aspetti dei contratti di vendita *online* e di altri tipi di vendita a distanza di beni[166], si integrerebbe con la Direttiva 2001/82/UE[167] e con quella 2000/31/CE[168] relative, rispettivamente, ai diritti dei consumatori ed al commercio elettronico. Essa stabilisce prescrizioni in merito alla conformità del contenuto digitale al contratto, ai rimedi che possono essere adottati dal consumatore in caso di difetto di conformità del contenuto digitale, alle modalità di esercizio dei predetti rimedi nonché in merito alle norme relative alla modifica ed alla risoluzione dei contratti di fornitura di contenuti digitali[169].

La proposta di direttiva si applica a qualsiasi contratto di fornitura di un contenuto digitale[170], indipendentemente dal supporto utilizzato per la sua trasmissione, con l'esclusione dei contratti concernenti: a) servizi nella cui

---

[166] *Cfr.* la precedente nota n. 163.

[167] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio del 25 ottobre 2011 sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio, reperibile su *eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX :32011L0083&rid=1*.

[168] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico), reperibile su *http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32000L0031&rid=1*.

[169] *Cfr.* art. 1, Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

[170] Per contenuto digitale si intende: *"a) i dati prodotti e forniti in formato digitale, ad esempio registrazioni audio o video, applicazioni, giochi digitali e qualsiasi altro tipo di software; b) un servizio che consente la creazione, il trattamento o la memorizzazione di dati in forma digitale, ove tali dati siano forniti dal consumatore, e c) un servizio che consente la condivisione di dati in formato digitale forniti da altri utenti del servizio e qualsiasi altra interazione con tali dati"*, così art. 2, Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

prestazione l'intervento del fornitore costituisce una componente predominante e il formato digitale costituisce solo un vettore; b) servizi di comunicazione elettronica ai sensi della Direttiva 2002/21/CE; c) servizi sanitari ai sensi dell'art. 3, lett. a, Direttiva 2011/24/UE; d) servizi di gioco d'azzardo che vengono forniti mediante strumenti elettronici su richiesta di un destinatario degli stessi servizi; e) servizi finanziari[171].

Alla fornitura del servizio deve corrispondere una controprestazione che può essere anche non pecuniaria e consistere nel consenso all'accesso ai dati personali o a qualsiasi altro dato a meno che la richiesta di accesso da parte del fornitore non sia giustificata da ragioni strettamente necessarie all'esecuzione del contratto o al rispetto di altri obblighi di legge[172].

La proposta di direttiva – che non pregiudica le disposizioni nazionali in materia contrattuale, quali, ad esempio, le norme sulla formazione e la validità dei contratti e sulla liceità del contenuto – impedisce agli Stati membri, a garanzia di una concreta armonizzazione, di adottare o mantenere in vita disposizioni divergenti rispetto a quelle dettate anche se tese a garantire al consumatore un diverso livello di tutela più o meno favorevole[173].

Il contenuto digitale deve essere conforme, per l'intera durata del rapporto, alle caratteristiche previste dal contratto quanto a funzionalità, interoperabilità, accessibilità, continuità e sicurezza e, inoltre, deve essere aggiornato ed idoneo

[171] *Cfr.* art. 3, Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.
[172] *Cfr.* art. 3, co. 4, Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.
[173] *Cfr.* art. 4, Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

ad ogni uso voluto dal consumatore e da questi portato a conoscenza del fornitore al momento della conclusione del contratto. Lo stesso prodotto digitale può essere fornito direttamente al consumatore o anche ad un terzo che, a sua volta, lo mette a disposizione del consumatore.

Nel caso in cui il contratto non definisce in modo chiaro e completo i requisiti del contenuto digitale, è necessario guardare agli scopi propri di un contenuto dalle medesime caratteristiche da individuare tenendo conto della controprestazione, di eventuali norme tecniche internazionali e di qualsiasi dichiarazione pubblica resa dal fornitore o da altre persone a monte della catena di operazioni commerciali[174].

In presenza di un contenuto integrato in modo errato nell'ambiente digitale[175] del consumatore, si presume la sussistenza di un difetto di conformità se l'integrazione è stata effettuata del fornitore oppure se l'errore è dipeso dalla carenza di istruzioni fornite al consumatore che ha eseguito l'integrazione.

Il contenuto digitale deve essere fornito al consumatore libero da qualsiasi diritto di terzi, inclusi quelli basati sulla proprietà intellettuale, così da consentire un uso conforme al contratto.

Sul fornitore grava l'onere della prova in merito alla conformità del contenuto al contratto fatte salve le ipotesi in cui riesce a dimostrare che

---

[174] Sugli aspetti da ultimo delineati *cfr.* gli artt. 5 e 6 della Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

[175] Per ambiente digitale – ai sensi dell'art. 2 della Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final* – si intende *"l'hardware, i contenuti digitali e le connessioni di rete, nella misura in cui siano sotto il controllo dell'utente"*.

"l'ambiente digitale del consumatore non è compatibile con i requisiti di interoperabilità e altri requisiti tecnici del contenuto digitale e nel caso in cui il fornitore abbia informato il consumatore di tali requisiti prima della conclusione del contratto". L'onere della prova graverà sul consumatore se quest'ultimo non collabora, per quanto gli è possibile, con il fornitore a circoscrivere il suo ambiente digitale[176].

Il fornitore è responsabile nei confronti del consumatore per la mancata fornitura del contenuto digitale e per qualsiasi difetto di conformità esistente al momento della fornitura e, comunque, per tutto il periodo di durata del rapporto. Dall'omessa fornitura, nei termini di cui all'art. 5 della proposta di direttiva, scaturisce il diritto del consumatore di recedere immediatamente dal contratto[177].

In presenza di difetti di conformità, il consumatore ha diritto al ripristino della stessa senza spese ed in un tempo ragionevole, sempre che ciò non sia *"impossibile, sproporzionato o illegale"*. In tal caso il consumatore ha diritto ad una riduzione del prezzo, proporzionale alla diminuzione di valore del contenuto digitale, o a recedere dal contratto.

Le stesse soluzioni si applicano quando il ripristino non è stato eseguito in un periodo di tempo ragionevole, quando lo stesso potrebbe arrecare un disagio notevole al consumatore nonché nell'ipotesi in cui il fornitore dichiara che non procederà al ripristino.

---

[176] *Cfr.*, con riferimento alle ultime questioni trattate, gli artt. 7, 8 e 9 della Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

[177] *Cfr.* artt. 10 e 11 della Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

Il recesso può aversi solo se il difetto di conformità *"compromette la funzionalità, l'interoperabilità e le altre principali prestazioni, quali l'accessibilità, la continuità e la sicurezza"* del contenuto digitale; l'onere di provare l'inesistenza della riferita compromissione è a carico del fornitore[178].

Il consumatore esercita il suo diritto alla risoluzione contrattuale inviando una comunicazione al fornitore che, conseguentemente, deve rimborsare, entro quattordici giorni dal ricevimento della predetta comunicazione, il prezzo pagato o astenersi dall'utilizzare la controprestazione non pecuniaria eseguita dal consumatore.

A seguito della risoluzione, inoltre, il fornitore deve mettere a disposizione del consumatore gli strumenti tecnici necessari a recuperare, gratuitamente e senza particolari disagi, tutti i contenuti forniti e *"gli eventuali altri dati prodotti o generati a seguito dell'utilizzo del contenuto digitale da parte del consumatore, nella misura in cui i dati siano stati conservati dal fornitore"*. Il consumatore, dal canto suo, deve astenersi dall'utilizzare o dal mettere a disposizione di terzi il contenuto digitale, procedendo ad eliminarlo o, comunque, a renderlo incomprensibile. Nel caso in cui il contenuto digitale è stato fornito su supporto durevole si deve procedere, entro quattordici giorni, alla restituzione dello stesso a spese del fornitore cancellando, al contempo, qualsiasi copia eventualmente disponibile[179].

---

[178] *Cfr.* art. 12 della Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

[179] *Cfr.* art. 13 della Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

Il consumatore, in ogni caso, ha diritto al risarcimento di qualsiasi danno subito al proprio ambiente digitale a causa di un difetto di conformità o della mancata fornitura del contenuto digitale.

La proposta di direttiva individua anche le ipotesi e le forme in cui il fornitore può apportare modifiche al contenuto digitale se il contratto prevede che lo stesso contenuto sia fornito per un periodo di tempo determinato. Laddove, invece, il contratto è a tempo indeterminato o, comunque, ha una durata superiore ai dodici mesi, il consumatore può recedere in qualsiasi momento dopo la prima scadenza annuale[180].

Il fornitore potrà agire in regresso nei confronti della persona o delle persone a monte della catena di operazioni commerciali quando la sua responsabilità verso il consumatore deriva da un atto o da un'omissione ascrivibile ad uno dei citati soggetti.

La proposta, infine, sancisce l'imperatività delle norme dettate escludendo la possibilità, per qualsiasi clausola contrattuale, di operare deroghe a danno del consumatore[181].

Nonostante l'apprezzabile sforzo compiuto nell'ottica della realizzazione di un mercato unico digitale, è opportuno rilevare un aspetto della proposta di direttiva che non sembra essere del tutto omogeneo con la Direttiva 2011/83/UE; in particolare, infatti, il concetto di contenuto digitale espresso nella proposta è più ampio di quello previsto dalla citata Direttiva 2011/83/CE

[180] Sugli aspetti da ultimo delineati, *cfr.* gli artt. 14, 15 e 16 della Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

[181] *Cfr.* artt. 17 e 21 della Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, 09.12.15, COM(2015) 634 *final*.

rendendo necessario un chiarimento teso a meglio delimitare l'ambito di operatività delle norme.

Il rilevato fermento normativo ed in generale l'attenzione prestata al fenomeno del *cloud computing*, fanno auspicare una reale armonizzazione in grado di ridurre l'incertezza giuridica percepita da imprese ed utenti.

Appare evidente, al contempo, che il massimo risultato si potrà ottenere solo quando l'attenzione e, quindi, la regolamentazione, sarà spostata dal piano Europeo al piano internazionale in considerazione della dimensione globale del *cloud*.

6.- *Il contratto di cloud computing e l'abuso di dipendenza economica nei rapporti B2b.*

Nell'analizzare i profili contrattuali del *cloud computing* non può omettersi un riferimento alle ipotesi in cui l'utente *cloud* non è un consumatore ma, piuttosto, un'impresa o un professionista.

La fornitura di servizi *cloud* nell'ambito di relazioni negoziali *business to business* (B2B) presuppone la necessità di prestare una particolare attenzione al contratto ed alle condizioni che regolano la responsabilità del fornitore del servizio. A tali tipi di rapporti, infatti, non è possibile applicare la disciplina di favore, a tutela del consumatore, in grado di neutralizzare clausole inique ed irragionevoli.

Gli utenti professionali, invero, pur essendo destinatari di una protezione affievolita rispetto alla categoria dei consumatori, non sono completamente privi di tutela rispetto alla stipula di clausole particolarmente penalizzanti.

In quest'ottica deve considerarsi la previsione di cui all'art. 9, l. 192/98[182] con cui è stato vietato l'abuso di dipendenza economica da intendersi come *"la situazione in cui un'impresa sia in grado di determinare, nei rapporti commerciali con un'altra impresa, un eccessivo squilibrio di diritti ed obblighi"*. L'abuso, inoltre, può consistere anche nel rifiuto di vendere o nel rifiuto di comprare, nell'imposizione di condizioni contrattuali ingiustificatamente gravose o discriminatorie nonché nell'interruzione arbitraria delle relazioni commerciali in atto.

La disciplina in esame, pur se inserita nella l. 192/98 in materia di subfornitura, ha carattere generale non riguardando solo gli abusi di dipendenza economica sorti nell'ambito di un rapporto di subfornitura ma, piuttosto, tutti i rapporti di cooperazione commerciale laddove sussistono le condizioni previste dal citato art. 9[183].

La dipendenza economica – in cui versa un'impresa, cliente o fornitrice, rispetto ad un'altra che si trova nella reale condizione di imporre alla controparte condizioni squilibrate a proprio esclusivo vantaggio – deve essere valutata considerando la reale possibilità, per il soggetto che subisce l'abuso, di reperire sul mercato valide soluzioni alternative rispetto a quelle offerte[184].

---

[182] V. l. 18 giugno 1998, n. 192, recante *Disciplina della subfornitura nelle attività produttive*.
[183] Sul punto, v. F. CARINGELLA, L. BUFFONI, *Manuale di diritto civile*, VI edizione, Roma, 2016, p. 1095.
[184] *Cfr.* V. PINTO, *L'abuso di dipendenza economica 'fuori dal contratto' tra diritto civile e diritto antitrust*, in *Riv. dir. civ.*, 2000, 394; G. OPPO, *Princìpi*, Torino, 2001, p. 43; A. MAZZIOTTI DI CELSO, *Abuso di dipendenza economica*, in *La Subfornitura, Commento alla legge 18 giugno 1998, n. 192*, G. ALPA – A. CLARIZIA, Milano, 1999, p. 247.

Il divieto sancito dall'art. 9 sanziona con la nullità il patto attraverso cui si realizza l'abuso di dipendenza economica[185]; si tratta di una nullità speciale di protezione atteso che la disciplina codicistica, prevista dall'art. 1421 c.c., consentendo a chiunque di invocare la nullità, mal si adatterebbe all'esigenza di tutelare l'imprenditore debole. Applicando l'art. 1421 c.c., infatti, ci si potrebbe trovare nell'assurda situazione in cui la stessa nullità è eccepita dalla parte contrattualmente forte che, abusando della sua posizione, è interessata a rendere nulla la pattuizione abusiva. Lo stesso giudice, inoltre, in virtù della richiamata disposizione, potrebbe rilevare d'ufficio la nullità anche nell'ipotesi in cui i conseguenti effetti non si realizzano a favore dell'imprenditore debole.

L'eccessivo squilibrio di diritti e obblighi che genera l'abuso di dipendenza economica può assumere rilevanza durante l'intera fase esecutiva ma anche in occasione della cessazione del rapporto. Nell'ambito dei contratti di *cloud computing*, ad esempio, potrebbero verificarsi ipotesi di abuso laddove il fornitore impedisse all'utente di trasferire i propri dati ad un altro *cloud provider* o condizionasse tale trasferimento al pagamento di costi molto rilevanti.

Tra le previsioni normative a tutela dell'imprenditore debole, infine, merita di essere ricordato l'art. 7, d.l. 1/12[186] che, modificando gli artt. 18 e 19, d.lgs.

[185] V. art. 9, co. 3, l. 192/98.
[186] V. d.l. 24 gennaio 2012 n. 1, recante *Disposizioni urgenti per la concorrenza, lo sviluppo delle infrastrutture e la competitività*, convertito in legge, con modificazioni, dall'art. 1, co. 1, l. 27/12.

206/05, ha esteso alle microimprese[187] la disciplina prevista per il consumatore contro le pratiche commerciali scorrette.

[187] Per microimprese – ai sensi dell'art. 18, co. 1, lett. d-*bis*), d.lgs. 206/05 – devono intendersi *"entità, società o associazioni che, a prescindere dalla forma giuridica, esercitano un'attività economica, anche a titolo individuale o familiare, occupando meno di dieci persone e realizzando un fatturato annuo oppure un totale di bilancio annuo non superiori a due milioni di euro, ai sensi dell'articolo 2, paragrafo 3, dell'allegato alla raccomandazione n. 2003/361/CE della Commissione, del 6 maggio 2003"*.

Capitolo IV
La tutela della *privacy* nei servizi di *cloud computing*

SOMMARIO: 1. Cloud *computing* e *privacy*: quadro normativo di riferimento; 2. Il *cloud computing*: ruoli e responsabilità nel trattamento dei dati; 3. Dalle misure minime di sicurezza al principio dell'*accountability*; 4. Lo *standard* ISO per il *cloud computing*; 5. Il trasferimento all'estero dei dati.

1.- *Cloud computing e privacy: quadro normativo di riferimento.*

La protezione dei dati personali, nell'ottica della loro sicurezza e riservatezza, rappresenta uno degli aspetti che desta maggiori preoccupazioni tra gli utenti del *cloud computing* incidendo sullo sviluppo dei relativi servizi[188].

Gli utenti, come già rilevato, sono attratti dalle indubbie potenzialità del *cloud* ma al tempo stesso sono spaventati dalla possibilità di perdere il controllo dei propri dati a causa della delocalizzazione delle risorse e del sempre più frequente trasferimento dei dati al di là dei confini nazionali.

In molti casi, inoltre, i fruitori del *web* si confrontano inconsapevolmente con il *cloud* senza avere alcuna cognizione della tecnologia su cui si poggia; ciò accade, il più delle volte, per l'estrema semplicità con cui è possibile accedere ai servizi utilizzando moduli di registrazioni *online* che fanno sottovalutare il riferito fenomeno di esternalizzazione dei dati. A ciò, inoltre, si

[188] Tra i contributi monografici più recenti v. F. PIROZZI, *Il cloud computing. Lex mercatoria e tutela dei dati*, Milano, 2016.

deve aggiungere che, spesso, le condizioni contrattuali, predisposte unilateralmente dal *provider*, omettono di riferire che i servizi erogati si basano su tecnologia *cloud* con relative implicazioni tecnico/giuridiche[189].

Nelle ipotesi di servizi SaaS l'utente immette i dati nella "nuvola" utilizzando l'interfaccia *software*; gestione, invio, archiviazione e memorizzazione degli stessi dati da parte del *cloud provider* costituiscono attività di trattamento[190]. Le stesse attività, inoltre, sono alla base dei servizi PaaS in cui il trattamento dei dati da parte del *provider* è finalizzato a consentire, da un lato, il funzionamento delle applicazioni realizzate e, dall'altro, la memorizzazione successiva di quanto prodotto con il loro utilizzo.

Nell'ambito dei servizi IaaS, infine, il *cloud provider*, mettendo a disposizione *hardware* e connettività, tratterà i dati oggetto di memorizzazione.

Il problema della sicurezza e della riservatezza dei dati è centrale per tutti i clienti dei servizi *cloud* ma lo è ancor di più per tutti coloro che ne fanno un uso professionale esponendosi, così, a responsabilità nei confronti di terzi clienti, fornitori e dipendenti, in caso di violazione delle disposizioni in materia di *privacy*.

L'utilizzo consapevole del *cloud*, pertanto, presuppone un'attenta valutazione delle condotte che l'utente può adottare a sua tutela nei confronti del *cloud provider* evitando, al contempo, responsabilità per illecito

---

[189] Sul punto, *cfr.* E. BELISARIO, *op. cit.*, p. 13 ss.

[190] Ai sensi dell'art. 4, co. 1, lett. a), d.lgs. 196/03, per trattamento di intende *"qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati"*.

trattamento dei dati di terzi a lui affidati e gestiti con sistemi di *cloud computing*.

È opportuno che l'utente verifichi, preliminarmente, se i dati immessi nel *cloud* sono trasferiti ed elaborati tramite *server* allocati in Italia, in Europa o, piuttosto, in un Paese extraeuropeo. Tale informazione è fondamentale per definire il livello di protezione assicurato agli stessi dati considerando, inoltre, che un trasferimento[191] in Paesi extraeuropei – se effettuato in spregio delle garanzie previste dalla disciplina in materia di protezione dei dati personali – costituisce un illecito trattamento.

Fondamentale importanza assume, ancora una volta, l'individuazione della legge applicabile ai rapporti tra utente e *cloud provider* in merito alla tutela dei dati personali.

Il quadro giuridico di riferimento, applicabile anche al *cloud computing*, è rappresentato dalla Direttiva 95/46/CE[192] recepita in Italia con il d.lgs. 196/03[193]. Si deve rilevare, da subito, che la predetta Direttiva è stata abrogata, con decorrenza dal 25 maggio 2018, dal Reg. UE 2016/679[194] pensato per

---

[191] Sul trasferimento dei dati all'estero, *cfr.* il successivo § 5.

[192] Direttiva 95/47/CE del Parlamento Europeo e del Consiglio, del 24.10.95, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, reperibile su *http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:31995L0046&from=it*.

[193] D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, reperibile su *www.garan-teprivacy.it/web/guest/home/docweb/-/docweb-display/export/1311248*.

[194] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, reperibile su *http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT*. Il Regolamento costituisce – unitamente alla Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*, reperibile su *http://eur-*

armonizzare le diverse norme nazionali in materia di *privacy*, riservando una particolare attenzione alle esigenze del mondo digitale ed al flusso dei dati personali.

Le nuove disposizioni, come si evidenzierà nel prosieguo, consentiranno di superare alcune criticità anche in merito alla tutela della *privacy* nei servizi di *cloud computing* che, per la loro complessa articolazione, si caratterizzano per peculiarità che mal si adattano alle previsioni della Direttiva 95/46/CE concepita in un periodo in cui i servizi digitali erano agli albori e la *rete internet* era utilizzata da una minima parte della popolazione europea.

La Direttiva 95/46/CE è stata recepita nel nostro Paese con il d.lgs. 196/03 che, sulla scorta di quanto previsto dalla disposizione europea, trova applicazione quando il *cloud provider* è stabilito in Italia o, in alternativa, quando lo stesso *provider* – stabilito in un territorio di un Paese non appartenente all'Unione Europea – utilizza, per il trattamento dei dati, strumenti situati in Italia, anche diversi da quelli elettronici, salvo l'ipotesi di utilizzo ai soli fini di transito nel territorio dell'Unione Europea[195].

Negli altri casi, quindi, anche quando gli utenti coinvolti sono soggetti di diritto italiani, o in senso più ampio europei, la disciplina non potrà trovare applicazione[196] con il conseguente rischio di minor tutela posto che le disposizioni *privacy* di molti paesi extraeuropei non offrono garanzie pari a quelle nazionali ed europee.

---

lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680&from=IT – il cd. *"pacchetto protezione dati personali"*.

[195] *Cfr.*, sul punto, art. 5, co. 1 e 2, d.lgs. 196/03.

[196] Si pensi, ad esempio, alla non rara ipotesi di servizio SaaS fornito da un *provider* americano, non stabilito in Italia, che utilizza, per il trattamento, strumenti non allocati in un Paese europeo.

L'utilizzo di criteri territoriali per la determinazione della legge applicabile, espone gli utenti *cloud* al rischio che il *cloud provider* possa aggirare i vincoli previsti dalla disciplina comunitaria in materia di protezione dei dati personali, spostando, semplicemente, la sede della società o i suoi *data center* fuori dall'Italia e dall'Europa.

Se è vero, quindi, che il *cloud provider*, con sede ed infrastrutture poste al di fuori dello Stato, non può essere assoggettato alla disciplina *privacy* è altrettanto vero che l'utente *cloud*, stabilito in Italia e titolare del trattamento[197] di dati di terzi a lui affidati e gestiti con servizi di *cloud computing*, dovrà adottare una condotta impeccabile, conforme alla normativa a tutela dei dati personali, per non incorrere nelle conseguenze previste per l'illecito trattamento[198].

Se persona fisica, l'utente *cloud,* che effettua un trattamento di dati per fini esclusivamente personali, non è soggetto all'applicazione del codice *privacy* fatte salve le ipotesi in cui i dati sono destinati ad una comunicazione sistematica o alla diffusione; devono applicarsi, in ogni caso, le disposizioni in tema di responsabilità e di sicurezza dei dati previste dagli artt. 15 e 31, d.lgs. 196/03.

Il Reg. UE 2016/679 ha introdotto un'importante novità che, garantendo l'applicazione della normativa *privacy* a prescindere dai riferiti criteri

[197] Sul ruolo che hanno nel trattamento dei dati, rispettivamente, i *cloud provider* e gli utenti *cloud*, *cfr.* il successivo § 2.

[198] A titolo esemplificativo, si consideri un'azienda italiana che decide di gestire in *cloud* i dati dei propri clienti e fornitori affidandosi ad un *provider* americano, non stabilito in Italia, che utilizza, per il trattamento, strumenti non allocati in un Paese europeo. L'azienda *de qua* sarà sempre titolare del trattamento e dovrà garantire, agli interessati, il rispetto del d.lgs. 196/03 pena la sua responsabilità.

territoriali, consente di superare alcune delle criticità segnalate. Le nuove disposizioni di tutela, infatti, si applicheranno anche *"al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare o da un responsabile del trattamento non stabilito nell'Unione"*, quando lo stesso trattamento è relativo all'offerta di beni o di servizi nell'UE o è finalizzato ad effettuare attività di monitoraggio (profilazione) del comportamento degli utenti all'interno dell'Unione[199].

2.- ***Il cloud computing: ruoli e responsabilità nel trattamento dei dati.***

In tutti i casi in cui l'utente *cloud* non è un semplice interessato al trattamento ma, piuttosto, un soggetto giuridico che gestisce, con servizi *cloud* e per esigenze professionali, dati di terzi a lui affidati, è importante definire il ruolo dallo stesso assunto anche per inquadrare meglio le relative responsabilità.

Come è noto, il d.lgs. 196/03 distingue il titolare, il responsabile e l'incaricato del trattamento; in particolare, il titolare è qualificato come il soggetto a cui *"competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"*, il responsabile come colui che è preposto *"dal titolare al trattamento di dati personali"* ed,

[199] *Cfr.* art. 3, co. 2, Reg. UE 2016/679. Si consideri, inoltre, che ai sensi del successivo comma 3, il regolamento *"si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico"*.

infine, l'incaricato come la persona fisica *"autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile"*[200].

Il responsabile del trattamento, che può essere un soggetto interno o esterno all'organizzazione del titolare, non ha autonomia di iniziativa ma agisce seguendo le indicazioni del titolare che vigila sulla puntuale osservanza delle istruzioni impartite e delle disposizioni in materia di trattamento anche con riferimento al profilo della sicurezza dei dati[201].

Tralasciando la figura dell'intermediario in ragione del suo ruolo marginale, è necessario capire se il *cloud provider* e l'utente *cloud* sono entrambi qualificabili come titolari (autonomi o contitolari) ovvero se, diversamente, il *cloud provider* deve essere considerato un responsabile esterno nominato dall'utente *cloud*, titolare, a sua volta, del trattamento dei dati di terzi gestiti con servizi di *cloud computing*.

La prima ipotesi può essere riscontrata ogni qual volta c'è un'effettiva libertà decisionale in merito al trattamento dei dati; in tal caso ci si dovrà confrontare prevalentemente con il problema del trasferimento all'estero dei dati personali[202].

La possibilità di qualificare il *cloud provider* come responsabile del trattamento, invece, presuppone l'effettività del controllo che il titolare è tenuto ad esercitare sul responsabile designato.

È difficile immaginare che ciò possa accadere in rapporti basati su contratti predisposti unilateralmente da soggetti tra cui, il più delle volte, sussistono

[200] *Cfr.* art. 4, co. 1, lett. f, g, h, d.lgs. 196/03.
[201] *Cfr.* art. 29, co. 5, d.lgs. 196/03.
[202] Sul punto, *cfr.* il successivo § 5.

gravi situazioni di squilibrio organizzativo, tecnologico ed economico che, di fatto, rendono impossibile un controllo reale.

Partendo da queste premesse, in ogni caso, sarà opportuno verificare, volta per volta, come si configura il rapporto che si crea tra il *cloud provider* e l'utente poiché la realtà prevarrà sempre sulle definizioni convenzionalmente utilizzate.

Dalla corretta attribuzione del ruolo di titolare e di responsabile del trattamento dei dati personali scaturiscono importanti conseguenze in relazione tanto alle responsabilità connesse al trattamento quanto alla liceità dello stesso.

La responsabilità per un trattamento illecito o per la mancata adozione di tutto quanto necessario e prescritto in tema di sicurezza, grava, almeno in prima battuta, sul titolare del trattamento in ragione del ruolo e del potere decisionale a lui attributo in merito alla gestione ed alla sicurezza dei dati.

Quest'ultimo, in caso di mancata adozione delle misure minime di sicurezza prescritte dal codice della *privacy*, è soggetto – ai sensi del combinato disposto degli artt. 33 e 169, d.lgs. 196/03 – all'arresto fino a due anni, salva la possibilità di estinguere il reato con la procedura prevista dal secondo comma dello stesso art. 169, d.lgs. 196/03. In ragione della formulazione della norma[203], è possibile immaginare che la predetta sanzione possa essere comminata anche al responsabile del trattamento laddove ometta di dare esecuzione alle istruzioni ricevute dal titolare.

[203] Si deve considerare, infatti, che l'art. 169, d.lgs. 196/03 si riferisce, genericamente, a *"chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 [...]"*. La disposizione, pertanto, lascia ampio spazio alla configurabilità di una responsabilità in capo ad un soggetto diverso dal titolare che, comunque, in virtù del richiamo all'art. 33, d.lgs. 196/03, è il principale destinatario della previsione.

L'illecito trattamento dei dati personali espone gli "interessati" al rischio di subire danni e pregiudizi di notevole entità. L'art. 15, co.1, d.lgs. 196/03 configura un'ipotesi di responsabilità aggravata collegata all'art. 2050 c.c. prevedendo che *"chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile"*. È, pertanto, necessario coordinare l'art. 15, co.1, d.lgs. 196/03 con l'art. 2050 c.c. secondo cui *"chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno"*.

L'equiparazione del trattamento dei dati personali all'esercizio di attività pericolosa di cui all'art. 2050 c.c., ha comportato l'alleggerimento dell'onere probatorio a carico del soggetto danneggiato rispetto a quanto previsto dell'art. 2043 c.c.; nell'ambito della tutela dei dati personali possono essere considerate *"misure idonee ad evitare il danno"* il rispetto delle prescrizioni del Garante, delle regole di trattamento, dei codici di deontologia e buona condotta nonché l'adozione delle misure minime di sicurezza previste dal d.lgs. 196/03.

L'interessato al trattamento, ai sensi dell'art. 15, co. 2, d.lgs. 196/03[204], può pretendere anche il risarcimento di danni non patrimoniali in tutte le ipotesi in cui sono state violate le condizioni di liceità del trattamento previste dall'art. 11, d.lgs. 196/03.

[204] *"Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11"*, così art. 15, co. 2, d.lgs. 196/03.

È possibile affermare, in definitiva, che l'interessato al trattamento – in virtù del combinato disposto degli artt. 15 ed 11, d.lgs. 196/03 e degli artt. 2050 e 2059 c.c. – può pretendere tanto il risarcimento dei danni patrimoniali quanto quello dei danni non patrimoniali.

Ricostruito il profilo della responsabilità civile per illecito trattamento dei dati personali, è opportuno individuare il soggetto tenuto a risarcire il danno; il tenore letterale dell'art. 15, co. 1, d.lgs. 196/03 potrebbe far ipotizzare che l'obbligo risarcitorio sarebbe configurabile in capo a *"chiunque"* e, quindi, indifferentemente in capo al titolare, al responsabile o all'incaricato del trattamento. Invero, però, si ritiene più corretta un'interpretazione restrittiva della citata norma con la conseguente configurabilità di un obbligo risarcitorio solo in capo al titolare o al responsabile, unici soggetti a determinare concretamente termini e modalità del trattamento, e quindi, in grado di fornire la prova che l'art. 2050 c.c. pone in capo al danneggiante[205].

In considerazione di quanto rappresentato e delle peculiarità del *cloud computing*, l'utente *cloud*, titolare del trattamento, per limitare la propria responsabilità, potrà contrattualmente specificare, in modo analitico, gli obblighi trasferiti al *cloud provider* responsabile del trattamento conservando e prevedendo adeguate modalità di controllo rispetto a quanto delegato.

Se, invece, il *cloud provider* è qualificato come titolare o contitolare del trattamento, l'utente dovrà fornire un'adeguata informativa agli interessati

[205] In capo all'incaricato potrebbe essere, al più, ipotizzata una responsabilità *ex* art. 2043 c.c. se, con il suo comportamento, danneggia l'interessato al trattamento.

procedendo, poi, ad un trasferimento dei dati in linea con le previsioni normative.

Il *cloud provider* nell'offrire i servizi contrattualizzati potrebbe sfruttare tecnologia *cloud* di terzi generando delle vere e proprie catene di fornitura; si pensi, ad esempio, all'ipotesi in cui la fruizione di servizi SaaS di un *provider* si basa su servizi IaaS di un terzo. In tal caso, come è facile comprendere, i dati degli interessati saranno trattati da un terzo soggetto che – se il *cloud provider* è qualificato come responsabile del trattamento – non potrà essere considerato né un incaricato del trattamento né un ulteriore responsabile del trattamento posto che il codice della *privacy* consente al solo titolare del trattamento di nominare uno o più responsabili[206].

In tali circostanze, onde evitare un trattamento illecito e le conseguenti responsabilità, l'utente *cloud* titolare del trattamento dovrà vincolare contrattualmente il *cloud provider* – responsabile del trattamento e che, a sua volta, intende affidarsi a servizi resi da terzi – ad avvalersi di soggetti disponibili ad essere designati come responsabili direttamente dal titolare.

Perché ciò accada, invero, sono necessarie delle condizioni preliminari che, in un modello di *cloud computing* "uno a molti" basato su clausole standardizzate, stenteranno ad avverarsi. Il *cloud provider*, infatti, dovrà indicare, all'utente *cloud* titolare del trattamento, tutti i riferimenti del terzo fornitore ed i luoghi in cui i dati vengono gestiti. Il terzo, a sua volta, dovrà accettare di essere nominato responsabile del trattamento assumendo nei

[206] *Cfr.* art. 29, co. 1, d.lgs. 196/03, secondo cui *"Il responsabile è designato dal titolare facoltativamente"*.

confronti del titolare gli stessi obblighi del *cloud provider*. Il tutto, ovviamente, dovrà avvenire nel rispetto della normativa in materia di *privacy* anche con riferimento all'eventuale trasferimento all'estero dei dati.

Le modifiche introdotte dal Regolamento UE 2016/679, consentiranno una semplificazione della procedura nell'ipotesi in cui il *cloud provider* è qualificato come responsabile del trattamento e si è in presenza di una catena di *cloud*. È stata prevista[207], infatti, la possibilità per il responsabile del trattamento di nominare, direttamente, un altro responsabile previa autorizzazione scritta, generale o specifica, del titolare del trattamento.

Quest'ultimo, in presenza di un'autorizzazione generale, dovrà essere informato di eventuali modifiche in merito all'aggiunta o alla sostituzione di altri responsabili potendo, eventualmente, opporsi alle stesse modifiche.

Le attività di trattamento di un responsabile devono essere disciplinate da un contratto o da altro atto giuridico, in linea con le previsioni del diritto dell'Unione o degli Stati membri, idoneo a fissare la durata del trattamento, la natura e la finalità dello stesso, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il documento – da stipulare in forma scritta, eventualmente, anche elettronica – dovrà prevedere, tra le altre cose, che il responsabile del trattamento *"a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento;*

[207] Sul punto, *cfr.* art. 28, Reg. UE 2016/679.

in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato"[208].

[208] Così art. 28, co. 3, Reg. UE 2016/679.

Il ricorso da parte di un responsabile ad un altro responsabile, per eseguire le istruzioni impartite dal titolare del trattamento, determina il dovere del primo di porre, in capo al secondo, gli stessi obblighi, in materia di protezione di dati personali, che lo legano al titolare prevedendo, in particolare, *"garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento"*.

Se il responsabile individuato in seconda battuta viola la disciplina in materia di protezione dei dati, il responsabile del trattamento nominato direttamente dal titolare manterrà, nei confronti di quest'ultimo, l'intera responsabilità per l'illecito trattamento[209].

Se il *cloud provider* e l'utente *cloud* sono entrambi qualificabili come titolari autonomi o contitolari del trattamento, come anticipato, ci si dovrà confrontare prevalentemente con la tematica del trasferimento all'estero dei dati personali[210]. È opportuno rilevare, infine, che ai sensi dell'art. 26, Reg. UE 2016/679, la contitolarità del trattamento si verifica nelle circostanze in cui due soggetti diversi determinano, congiuntamente, le finalità ed i mezzi del trattamento. Le rispettive responsabilità devono essere determinate con un chiaro accordo recante l'indicazione delle modalità di esercizio dei diritti dell'interessato e di comunicazione delle informazioni di cui agli artt. 13 e 14, fatte salve le ipotesi in cui le stesse responsabilità sono determinate dal diritto dell'Unione o dello Stato membro di appartenenza dei titolari del trattamento;

---

[209] Si deve tener presente, infine, che, ai sensi dell'art. 28, co. 10, Reg. UE 2016/679, *"fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione"*.

[210] Sul punto, *cfr.* il successivo § 5.

l'interessato, in ogni caso, potrà far valere i propri diritti *"nei confronti di e contro ciascun titolare del trattamento"*.

3.- *Dalle misure minime di sicurezza al principio dell'accountability.*

La normativa *privacy* attualmente in vigore[211] prescrive, al titolare del trattamento, l'adozione di un duplice livello di tutela a protezione dei dati personali, costituito da misure minime di sicurezza, previste dagli artt. 34, 35, 36, d.lgs. 196/03 e dall'allegato B allo stesso d.lgs. 196/03, nonché da tutte le misure idonee ad evitare il danno che, a differenza delle prime, non sono predeterminate dal legislatore ma, piuttosto, devono essere identificate in ragione del contesto operativo e tecnologico in cui operano tanto il *cloud provider* quanto l'utente *cloud*.

Il Codice della *privacy*, con riferimento alle misure minime, distingue tra quelle a tutela del trattamento di dati personali effettuato con strumenti elettronici[212] e quelle a tutela del trattamento effettuato senza l'ausilio di tali strumenti[213].

L'allegato B precisa, in relazione al trattamento effettuato con strumenti elettronici, che le misure minime di sicurezza devono essere adottate dal titolare, dal responsabile e, ove designato, dall'incaricato.

In presenza di condizioni standardizzate per la fornitura di servizi *cloud*, l'utente *cloud* non ha margini per incidere sulle misure minime che, pertanto,

---

[211] È opportuno ricordare che la Direttiva 95/46/CE, recepita in Italia con il d.lgs. 196/03, è stata abrogata, con decorrenza dal 25 maggio 2018, dal Reg. UE 2016/679.
[212] V. art. 34, d.lgs. 196/03.
[213] V. art. 34, d.lgs. 196/03.

dovranno essere verificate preventivamente alla stipula del contratto per accertare la loro rispondenza alla normativa *privacy*.

La responsabilità dell'utente *cloud*, titolare del trattamento, in merito all'implementazione ed alla gestione delle misure minime di sicurezza, cambia al variare della tipologia di servizio *cloud*. In presenza di un *cloud provider* qualificato come responsabile del trattamento è opportuno, pertanto, regolare contrattualmente tutti quegli aspetti che non ricadono automaticamente sotto la gestione del titolare.

L'adozione delle misure minime di sicurezza elimina il rischio di incorrere in sanzioni amministrative e penali; per evitare la responsabilità civile *ex* art. 15, d.lgs. 196/03 sarà necessario, inoltre, predisporre tutte le misure idonee a ridurre al minimo *"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"*[214]. In questo caso, come già sottolineato, è stato indicato l'obiettivo da raggiungere ma non le misure tipo da adottare che, invece, vanno individuate nell'ambito di un più generale processo di valutazione dei rischi, in occasione del quale devono essere considerate le specifiche implicazioni connesse all'utilizzo di soluzioni di *cloud computing*.

Dall'analisi dei rischi potrà scaturire la necessità di adottare, a garanzia dei dati personali, non solo misure tecnologicamente avanzate ma anche misure organizzative ed interventi formativi da definire contrattualmente tra i soggetti protagonisti del trattamento.

[214] V. art. 31, d.lgs. 196/03.

Con il Reg. UE 2016/679 è cambiato l'approccio rispetto alle misure di sicurezza: si è optato per un modello basato sulla cd. *accountability*[215] rispetto all'attuale sistema legato ad adempimenti formali a cui sono ricollegate responsabilità civili, penali ed amministrative.

Il regolamento mira ad una tutela sostanziale dei dati; il titolare del trattamento deve adottare un complesso di misure giuridiche, tecniche ed organizzative per la protezione dei dati personali ed essere in grado, conseguentemente, di dimostrare che gli accorgimenti da lui adottati garantiscono un trattamento sicuro e conforme allo stesso regolamento. Le misure – che andranno aggiornate e riesaminate ogni qual volta è necessario – dovranno tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi per i diritti e per le libertà delle persone fisiche[216].

Il principio di *accountability* è strettamente legato all'analisi del rischio, alla valutazione di impatto sulla protezione dei dati ed ai principi di *"privacy by default"* e di *"privacy by design"* che devono essere presenti nella progettazione di servizi e programmi.

Il legislatore europeo, con l'art. 32 del Reg. UE 2016/679, ha previsto che le misure tecniche ed organizzative adottate dal titolare e dal responsabile del trattamento devono garantire un livello di sicurezza adeguato al rischio da

[215] Con tale definizione ci si riferisce alla responsabilizzazione del titolare del trattamento a cui è lasciata un'ampia autonomia nella definizione delle modalità di tutela dei dati trattati. L'attuale sistema, invece, è basato su una stringente disciplina che regola nel dettaglio i comportamenti da porre in essere, lasciando poca autonomia decisionale al titolare che deve per lo più adeguarsi al modello predefinito. Il concetto di *accountability* è precedente allo stesso Reg. UE 2016/679; il Gruppo di lavoro art. 29, infatti, si è soffermato su tale tematica già nel 2010 con il parere n. 3, reperibile su *http://ec.europa.eu/justice/policies/privacy/docs /wpdocs/2010/wp173_it.pdf*.

[216] Sul punto, *cfr.* art. 24, Reg. UE 2016/679.

valutare *"tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche [...]"*. In particolare, pur in presenza di un'ampia libertà di scelta tra le soluzioni più adeguate, nell'individuare le misure da adottare si devono tenere in considerazione quelle che comprendono *"a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento"*[217].

La valutazione d'impatto, a sua volta, costituisce uno strumento fondamentale per valutare lo stato del proprio sistema di gestione dei dati personali ed i relativi margini di miglioramento. L'indagine dovrà soffermarsi, tra l'altro, sulle *"misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione"*[218].

[217] Così art. 32, co. 1, lett. a - d, Reg. UE 2016/679.
[218] *Cfr.* art. 35, Reg. UE 2016/679.

Il Regolamento, inoltre, ha introdotto anche il concetto di *privacy by default* che consiste nell'obbligo, per il titolare del trattamento, di predisporre misure tecniche ed organizzative che per impostazione predefinita, di *default*, consentano di trattare, per un periodo determinato, solo i dati personali strettamente necessari per una specifica finalità preservandoli da accessi indiscriminati da parte di un numero indefinito di persone fisiche[219]. Per *privacy by design*, invece, si intende, la necessità di adottare soluzioni che, *"sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso"*, garantiscano il rispetto della disciplina regolamentare nonché la tutela dei diritti degli interessati[220].

Il titolare del trattamento, nell'ottica dell'*accountability*, può dimostrare, di aver effettuato una gestione dei dati in linea con la normativa *privacy*, attraverso l'adozione delle misure di sicurezza, l'adesione ai Codici di condotta[221] o attraverso il ricorso ai meccanismi di certificazione previsti dal regolamento[222].

[219] V. art. 25, co. 2, Reg. UE 2016/679.
[220] *Cfr.* art. 25, c. 1, Reg. UE 2016/679. Un primo approccio al concetto di *privacy by design* può essere rinvenuto anche nell'art. 3, d.lgs. 196/03, secondo cui *"i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità"*.
[221] Sul punto, v. art. 40 e 41, Reg. UE 2016/679.
[222] V. art. 42, Reg. UE 2016/679.

4.- *Lo standard ISO per il cloud computing.*

L'*International Organization for Standardization* (ISO) in cooperazione con l'IEC (*International Electrotechnical Commission*)[223], ha pubblicato, nell'agosto del 2014, l'ISO/IEC 27018:2014[224] che, basandosi sugli *standard* ISO 27001 e 27002, raccoglie un insieme di regole elaborate per garantire la tutela dei dati personali da parte dei *public cloud provider* che si adeguano allo stesso *standard* ISO 27018. Attraverso un approccio orientato al concetto di *privacy by design*, infatti, si è cercato di far fronte alle diverse questioni giuridiche connesse alla gestione dei dati personali nel *public cloud*.

L'elaborazione dello *standard* in esame è stata incentivata dai Garanti *Privacy* che, riuniti nel gruppo *ex* art. 29[225], hanno rilevato il rischio per gli utenti *cloud*, titolari del trattamento, *"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, la trasparenza, l'isolamento, la portabilità dei dati e la possibilità di intervento sugli stessi"*.

---

[223] L'*International Organization for Standardization* è un'organizzazione internazionale non governativa, con sede a Ginevra, che include gli organismi nazionali per la definizione degli *standard*; la presenza dell'Italia all'interno della stessa organizzazione è assicurata dall'Ente Nazionale Italiano di Unificazione (UNI) che partecipa all'attività normativa ISO. L'obiettivo perseguito è quello di fissare le specifiche tecniche di prodotti, servizi e sistemi, per garantire qualità, sicurezza ed efficienza facilitando, in tal modo, anche i rapporti commerciali internazionali. In ragioni dei numerosi settori di intervento, l'*International Organization for Standardization* si avvale di comitati di esperti composti da membri nominati su segnalazione degli organismi nazionali associati.
L'ISO collabora costantemente con l'IEC (*International Electrotechnical Commission*) a sua volta deputata alla definizione degli *standard* in materia di elettronica, elettricità e tecnologie collegate.

[224] ISO/IEC 27018:2014, *Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*, reperibile a pagamento su *http://www.iso.org/iso/catalogue_detail.htm?Csnumber=61498*.

[225] Il riferimento, come già precisato, è all'art. 29, Direttiva 1995/46/CE, che ha istituito il *"Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali"* regolandone il funzionamento.

Contestualmente, è stata evidenziata l'opportunità di appurare, preventivamente, l'affidabilità e la credibilità del *provider*, rispetto all'adempimento degli obblighi *privacy*, anche attraverso *"la verifica o la certificazione indipendente effettuata da un terzo affidabile"*[226].

Lo sviluppo di uno *standard* per la certificazione dei servizi *cloud* è in linea, inoltre, con gli obiettivi comunitari evidenziati nel documento relativo alla necessità di sfruttare il potenziale del *cloud computing* in Europa[227].

L'ISO 27018, pertanto, si inserisce perfettamente nel quadro delineato ed è pienamente compatibile anche con il successivo Reg. UE 2016/679 avendone anticipato, tra l'altro, una serie di soluzioni a garanzia della *privacy* e della sicurezza dei dati nel pieno rispetto del principio della *cd. accountability*.

Lo *standard* ISO 27018, come già precisato, si caratterizza per un *quid pluris* rispetto alle ISO 27001 e 27002 da cui prende le mosse. In particolare, l'ISO 27001 stabilisce requisiti generici che devono essere posseduti, dai soggetti certificati, a garanzia della sicurezza delle informazioni presenti nei loro sistemi informatici.

In applicazione dell'ISO 27002, invece, gli stessi soggetti certificati – a seguito di una mirata analisi dei rischi connessi all'utilizzo dei sistemi informatici – definiscono specifiche attività di controllo elaborando soluzioni

[226] Gruppo di lavoro articolo 29 per la protezione dei dati, Parere 05/2012 sul *cloud computing*, p. 7 e 24, reperibile su *ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_it.pdf*

[227] V. Comunicazione della Commissione Europea al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Sfruttare il potenziale del cloud computing in Europa*, 27.09.12, COM(2012) 529 final, reperibile su *http://ec.europa.eu /transparency/regdoc/rep/1/2012/IT/1-2012-529-IT-F1-1.Pdf*.

in grado di garantire la sicurezza organizzativa, la gestione della continuità operativa nonché la verifica degli accessi e la sicurezza del personale.

Il *cloud provider*, muovendo da questi presupposti, per essere in linea con l'ISO 27018 ed ottenere il relativo riconoscimento, deve garantire: a) all'interessato la possibilità di far valere, nei confronti dell'utente titolare del trattamento, i diritti a lui riconosciuti dalla normativa *privacy* anche se i suoi dati sono gestiti in *cloud*. Il *provider* responsabile del trattamento, infatti, dovrà mettere a disposizione del titolare, strumenti in grado di assicurare l'esercizio dei diritti dei soggetti i cui dati sono trattati; b) la rispondenza degli strumenti con cui è effettuato il trattamento a quelli indicati nella *privacy policy* comunicata all'utente sin dall'inizio del rapporto. Laddove si rende necessario, per ragioni tecniche, procedere ad una sostituzione dei predetti strumenti, l'utente deve poter opporsi alla modifica risolvendo, eventualmente, il vincolo contrattuale; c) un trattamento dei dati in *cloud* non finalizzato ad attività pubblicitarie o di *marketing* diretto, a meno che non ci sia l'espresso consenso dell'interessato che, in ogni caso, non può costituire un presupposto a cui subordinare la fruizione del servizio *cloud*; d) la possibilità di conoscere, da subito, l'esistenza di eventuali catene di *cloud*. All'utente titolare del trattamento, inoltre, deve essere concesso il diritto di opporsi ad eventuali modifiche della stessa catena; e) la tempestiva comunicazione di eventuali violazione dei dati personali (cd. *data breaches*) per consentire, all'utente titolare del trattamento, di informare l'Autorità di controllo ed i soggetti interessati nei tempi previsti dalla legge; f) l'adozione di idonee procedure per la restituzione, il trasferimento o la cancellazione dei dati detenuti dal *cloud*

provider a conclusione del rapporto contrattuale; g) una documentabile verifica periodica della conformità dei servizi offerti agli *standard* di sicurezza; h) l'adeguata formazione del personale impiegato da vincolare a patti di riservatezza.

I fornitori dei servizi *cloud* non sono obbligati ad adeguarsi all'ISO 27018 né a recepire, nelle condizioni contrattuali, le relative previsioni. Lo *standard* costituisce, in ogni caso, un'importante strumento per verificare la posizione del *cloud provider* rispetto agli obblighi in materia di *privacy*.

La norma ISO 27018 che impone al *cloud provider* di comunicare senza ritardo, all'utente, l'eventuale violazione dei dati in *cloud*, ha anticipato quanto previsto dall'art. 34, Reg. UE 2016/679[228], rubricato *"comunicazione di una violazione dei dati personali all'interessato"*, costituendone, invero, il presupposto applicativo in ambito *cloud*.

Il citato articolo, infatti, ha introdotto l'obbligo per il titolare del trattamento di comunicare all'interessato la violazione dei dati personali quando la stessa è idonea ad arrecare un elevato pregiudizio ai diritti ed alle libertà delle persone fisiche[229]. L'utente *cloud*, titolare del trattamento, quindi, non sarà in grado

[228] Con tale norma è stato generalizzato l'obbligo, per tutti di tutti i titolari del trattamento, di comunicare agli interessati la violazione dei dati personali. Sino al Reg. UE 2016/679, infatti, il predetto obbligo era posto – ai sensi della Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, reperibile su *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:it:PDF* – solo in capo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico.

[229] La comunicazione all'interessato non è necessaria se – ai sensi dell'art. 34, co. 3, Reg. UE 2016/679 – è soddisfatta una delle seguenti condizioni *"a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si*

assolvere al predetto obbligo di comunicazione se, a sua volta, non riceve evidenza della violazione da parte del *cloud provider* responsabile dello stesso trattamento. Ci sarà, invece, perfetta coincidenza tra lo *standard* e la citata previsione regolamentare nell'ipotesi in cui il *provider* è qualificato come titolare del trattamento; in tal caso, quest'ultimo dovrà procedere direttamente ad effettuare la comunicazione ai soggetti interessati i cui dati sono stati violati.

Si ritiene opportuno, per completezza espositiva, evidenziare che l'art. 33, Reg. UE 2016/679 ha previsto, altresì, l'obbligo del titolare del trattamento di notificare[230] l'eventuale violazione dei dati personali all'Autorità di controllo; non sarà necessario procede in tal senso, nelle ipotesi in cui, la stessa violazione, non presenta rischi per i diritti e le libertà delle persone fisiche coinvolte.

L'adeguata verifica del rispetto della previsione in esame, presuppone la meticolosa documentazione di ogni violazione *"comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio"*.

L'ISO 27018 ha previsto, come anticipato, la necessità, per il *cloud provider*, di adottare un'adeguata *policy* di *transfer back*. In questa stessa direzione si è mosso anche il legislatore europeo che, normando il diritto alla

---

procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia".

[230] Ai sensi dell'art. 33, co. 3, Reg. UE 2016/679, la notifica deve almeno *"a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi"*.

portabilità dei dati[231], ha esteso a tutti i "trattamenti" un principio originariamente pensato per il *cloud*. L'interessato può chiedere al titolare del trattamento una copia dei dati personali che lo riguardano in un *"formato strutturato, di uso comune e leggibile da dispositivo automatico"* e, inoltre, può trasferire gli stessi dati, senza alcun impedimento, ad un altro titolare.

Il diritto alla portabilità può essere esercitato se il trattamento è effettuato con mezzi automatizzati, se si basa sul consenso prestato dall'interessato, all'occorrenza esplicitamente, per una o più finalità specifiche o, se lo stesso, è necessario all'esecuzione di un contratto.

Il Gruppo dei Garanti UE[232] ha evidenziato, con le *"guidelines on the right to data portability"*[233], l'importanza del diritto alla portabilità nell'ottica di un'effettiva libertà di scelta dell'interessato che può decidere di trasferire altrove i propri dati. Con il citato documento sono stati analizzati, inoltre, gli aspetti tecnici relativi all'esigenza di garantire l'interoperabilità tra i sistemi, anche con lo sviluppo di specifiche soluzioni informatiche, per dare piena attuazione al diritto.

In definitiva ed in considerazione di quanto sino ad ora precisato, è evidente l'importanza assunta dallo *standard* ISO 27018 a garanzia di un trattamento in linea con le previsioni normative e con le esigenze di tutela dei dati in *cloud*.

---

[231] V. art. 20, Reg. UE 2016/679.

[232] Il Gruppo dei Garanti UE, *ex* art. 29, Direttiva 95/46/CE, sarà sostituito – a decorrere dal 28.05.18, data di abrogazione della stessa Direttiva 95/46/CE – dal Comitato europeo per la protezione dei dati previsto dal Reg. UE 2016/679.

[233] Gruppo di lavoro articolo 29 per la protezione dei dati, 13.12.16, *Guidelines on the right to data portability*, reperibile su *http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf*.

5.- ***Il trasferimento all'estero dei dati.***

Il tema del trasferimento dei dati all'estero assume particolare importanza nell'ambito dei servizi di *cloud computing* poiché, come già precisato, è frequente che il loro funzionamento è basato su flussi transfrontalieri di dati verso Paesi esteri ove sono situati i *server* dei *cloud provider*.

La circolazione dei dati all'interno dell'Unione Europea è libera[234] e, conseguentemente, non può essere opposto nessun limite al loro trasferimento se i *server* del *cloud provider* sono collocati nel territorio dell'Unione.

Il d.lgs. 196/03, ribadendo il principio europeo di libera circolazione dei dati, fa salva la possibilità di adottare provvedimenti in grado di incidere su tale libertà, quando il trasferimento è posto in essere per eludere la normativa italiana eventualmente più rigorosa di quella di un altro Stato membro[235]. In tali circostanze, però, come opportunamente osservato[236], è necessario che alla base del trasferimento ci sia esclusivamente una finalità elusiva.

Il legislatore italiano, recependo la direttiva comunitaria, ha previsto specifiche regole per il trasferimento extraeuropeo di dati personali a maggior tutela degli interessati al trattamento.

In particolare, il predetto trasferimento è consentito quando è autorizzato dal Garante previa verifica dell'esistenza di adeguate garanzie individuate con le

---

[234] V. la Direttiva 95/46/CE, art. 1, co. 2, secondo cui *"gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1*". Nello stesso senso si è espresso il Reg. UE 2016/679, art. 1, co. 3, precisando che *"la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali"*.

[235] Sul punto, v. art. 42, d.lgs. 196/03.

[236] V. G. FINOCCHIARO, *Privacy e protezione dei dati personali, Disciplina e strumenti operativi*, Bologna, 2012, p. 282.

decisioni previste dagli artt. 25, co. 6,[237] e 26, co. 4[238], della Direttiva 95/46/CE *"con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti"*[239].

La Commissione europea compie la sua valutazione sull'adeguatezza del livello di protezione assicurato da un Paese terzo, considerando tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati soffermandosi, nello specifico, sulla natura dei dati, sulle finalità del o dei trattamenti previsti, sulle norme di diritto vigenti nel Paese di destinazione nonché sulle regole professionali e sulle misure di sicurezza ivi osservate[240].

Gli Stati non comunitari che, sino ad ora, secondo la Commissione, garantiscono un'adeguata protezione dei dati personali sono Andorra, Israele, Argentina, Canada, Faer Oer, Isola di Guernsey, Isola di Man, Jersey, Nuova Zelanda, Svizzera, Uruguay[241].

---

[237] Ai sensi dell'art. 25, co. 6 della Direttiva 95/46/CE *"la Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un Paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona"*.

[238] L'art. 26, co. 4, Direttiva 95/46/CE prevede che *"qualora la Commissione decida, secondo la procedura di cui all'articolo 31, paragrafo 2, che alcune clausole contrattuali tipo offrono le garanzie sufficienti di cui al paragrafo 2, gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione"*.

[239] V. art. 44, co. 1, lett. b, d.lgs. 196/03.

[240] Sul punto, *cfr.* art. 25, co. 2, Direttiva 95/46/CE. È opportuno precisare che la decisione della Commissione è assunta sulla scorta di un procedimento che prevede, fra l'altro, il parere favorevole del Gruppo dei Garanti UE, *ex* art. 29, Direttiva 95/46/CE.

[241] Le decisioni di adeguatezza della Commissione europea sono reperibili su *www.garante privacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/ trasferimento-dei-dati-verso-paesi-terzi*. Le autorizzazioni del Garante per il trasferimento verso paesi terzi, invece, sono reperibili su *www.garante privacy.it/web/guest/home/ricerca? p_p_id=searchportlet_WAR_labcportlet&p_p_lifecycle=0*.

L'eventuale trasferimento dei dati verso *server* localizzati negli Stati Uniti presuppone l'adesione[242], da parte del *provider* statunitense, all'accordo *EU-US Privacy Shield*[243] che ha sostituito quello noto come *Safe Harbour*[244] dichiarato invalido dalla Corte di Giustizia dell'Unione Europea[245] perché caratterizzato da un livello di protezione dei dati inferiore a quello previsto nel territorio dell'Unione.

Il nuovo accordo – frutto di un intenso dialogo tra la Commissione e le Autorità statunitensi teso ad una nuova decisione sull'adeguatezza, rispondente ai requisiti dell'art. 25, Direttiva 95/46/CE, da valutare sulla scorta della decisione della Corte di Giustizia – ha introdotto nuovi obblighi per le imprese americane che trattano dati personali di cittadini europei. Queste ultime dovranno autocertificare annualmente il rispetto degli obblighi scaturenti dal *Privacy Shield*, pubblicare sul proprio sito *internet* una *privacy policy*, rispondere tempestivamente ai reclami e, da ultimo, collaborare con le Autorità Garanti Europee dando seguito alle loro richieste. Per la prima volta, inoltre,

---

[242] L'adesione all'accordo deve risultare da specifica documentazione che le imprese americane devono consegnare agli organi competenti.

[243] Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la *privacy*, reperibile su *http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016 D1250&from=IT*. Il Garante della *privacy*, con provvedimento del 27.10.16, n. 436 (doc. web n. 5652873), reperibile su *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/5652873*, ha autorizzato il trasferimento di dati all'estero tramite il predetto accordo denominato *EU-U.S. Privacy Shield*.

[244] Decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "Domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, reperibile su *http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32000D0520&from=IT*.

[245] V. Corte di giustizia dell'Unione Europea del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems* vs. *Data Protection Commissioner*, reperibile su *http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=IT*.

gli USA hanno formalmente escluso il controllo indiscriminato e di massa dei dati trasferiti accettando la revisione annuale dell'accordo finalizzata alla verifica della sua efficacia con l'intervento di esperti dei servizi di sicurezza americani e delle diverse Autorità europee per la protezione dei dati. La Commissione europea, sulla scorta di tale revisione, relazionerà annualmente al Parlamento ed al Consiglio.

Sono stati previsti, infine, diversi meccanismi per la risoluzione di eventuali controversie. I cittadini europei, infatti, hanno la possibilità di far valere i loro diritti a) rivolgendosi direttamente all'impresa che avrà quarantacinque giorni di tempo per rispondere al reclamo presentato dall'interessato; b) utilizzando un meccanismo gratuito di *Alternative dispute resolution* (ADR); c) rivolgendosi alla propria Autorità garante che potrà contare sulla collaborazione del *Department of Commerce* e della *Federal Trade Commission* per compiere verifiche sui reclami pendenti con l'obiettivo di giungere ad una rapida definizione; d) rivolgendosi al *Privacy Shield Panel* per ottenere una soluzione sulla base di un meccanismo arbitrale.

Il trasferimento dei dati verso Paesi extraeuropei che non garantiscono un adeguato livello di protezione dei dati personali può avvenire, come anticipato, sulla base di clausole contrattuali che, secondo una decisione della Commissione Europea, tutelano adeguatamente i diritti dell'interessato.

Il Garante della *privacy*, con deliberazione del 27 maggio 2010[246], ha autorizzato i trasferimenti verso Stati non appartenenti all'Unione quando gli

[246] Autorizzazione al trasferimento di dati personali del territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuato in conformità alle clausole contrattuali tipo, di cui all'allegato alla decisione della Commissione europea del 5 febbraio 2010, n. 2010/87/UE, 27

stessi sono effettuati in conformità alle clausole tipo, individuate dalla Commissione con la decisione 2010/87/CE[247], che offrono sufficienti garanzie per la tutela della vita privata, dei diritti e delle libertà fondamentali dei soggetti i cui dati sono trattati.

La predetta decisione contiene, tra l'altro, specifiche clausole contrattuali che regolano le ipotesi in cui un responsabile del trattamento extraeuropeo, che gestisce i dati nell'interesse di un titolare stabilito nell'Unione, affida il trattamento ad un altro soggetto di un Paese terzo che non offre un adeguato sistema di protezione. In tal caso, è necessario il preventivo consenso scritto del titolare ed uno specifico subcontratto[248] che deve vincolare il subincaricato al rispetto degli obblighi assunti dal responsabile sulla base delle clausole *standard*.

Il titolare, a sua volta, deve tenere a disposizione dell'Autorità di controllo un elenco aggiornato dei subcontratti che il responsabile è tenuto ad inviare all'atto della loro conclusione[249].

In ragione di quanto sopra precisato, quindi, in presenza di un *cloud provider* stabilito fuori del territorio dell'Unione, in un Paese che non offre protezione adeguata, il contratto con l'utente *cloud* titolare del trattamento, deve necessariamente recepire le clausole tipo previste dalla decisione

---

maggio 2010, doc. *web* n. 1728496, reperibile su *http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1728496*.

[247] Decisione 2010/87/CE relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, reperibile su *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:IT:PDF*.

[248] Il subincaricato, in ragione di quanto previsto dalla clausola n. 1, paragrafo 1, decisione 2010/87/CE, potrà anche limitarsi a sottoscrivere il contratto concluso tra il titolare ed il responsabile del trattamento.

[249] Sul punto, *cfr.* clausola n. 5, lett. j, e clausola n. 11, paragrafo 4, decisione 2010/87/CE.

2010/87/UE anche con riferimento all'eventuale trasferimento effettuato dal *provider* ad altro subincaricato; in difetto, il trattamento sarà illegittimo con tutte le conseguenze di legge.

Il d.lgs. 196/03 prevede, inoltre, che il trasferimento dei dati personali verso un Paese *extra* UE è consentito, altresì, quando il Garante lo autorizza sulla base di adeguate garanzie per l'interessato *"[...] prestate con un contratto o mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo [...]"*[250]. Da tale previsione normativa traggono efficacia le *cd. Binding corporate rules* (BCR)[251] che permettono il libero trasferimento dei dati all'interno di società appartenenti allo stesso gruppo d'imprese. Si tratta, nello specifico, di un documento soggetto all'autorizzazione del Garante dietro espressa richiesta della società interessata.

Il testo delle BCR deve essere predisposto sulla base della disciplina nazionale ed europea in materia di protezione dei dati personali nonché dello schema elaborato dal Gruppo dei Garanti Europei[252]. Il trattamento è da effettuare nel rispetto dei principi di correttezza e legittimità, di finalità, necessità e proporzionalità; il titolare deve fornire l'informativa all'interessato, adottare idonee misure di sicurezza e garantire il risarcimento del danno

[250] V. art. 44, co. 1, lett. a, d.lgs. 196/03.
[251] In argomento, v. G. FINOCCHIARO, *op. cit.*, p. 287 ss.
[252] V. Gruppo dei Garanti europei *ex* art. 29, 03.06.2003, Documento di lavoro n. 74, doc. *web* n. 1609361, Trasferimenti di dati personali ai paesi terzi: applicazione dell'Articolo 26 (2) della Direttiva Europea sulla protezione dei dati alle *Binding Corporate Rules* (Norme d'impresa vincolanti) per il trasferimento internazionale di dati, reperibile su *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1609361* nonché ID., 24.06.08, Documento di lavoro n. 153, doc. *web* n. 1607808, che presenta uno schema di elementi e principi delle *Binding Corporate Rules*, reperibile su *www.garanteprivacy.it/web /guest/home/docweb/-/docweb-display/export /1619530*.

eventualmente prodotto dal mancato rispetto delle BCR. La loro fruizione presuppone, inoltre, l'adeguata formazione del personale in materia di *privacy* e la creazione di una rete di responsabili dedicata ai reclami degli interessati grazie ad un meccanismo di gestione del contenzioso appositamente implementato, nonché al monitoraggio del rispetto delle regole da parte di tutti i soggetti del gruppo.

La procedura per ottenere l'approvazione delle BCR è piuttosto complessa e si articola in una fase europea ed una fase nazionale.

Per l'adozione di un testo condiviso è necessaria la collaborazione, sulla base del modello predisposto dal Gruppo dei Garanti *ex* art. 29[253], di tutte le Autorità di protezione dei dati personali dei singoli Stati membri da cui hanno origine i trasferimenti infragruppo *extra* UE.

La società capogruppo dialoga con la *cd. lead Autority* che, in rappresentanza di tutte le *Data Protection Autorities* e con il supporto di due di esse, ha il compito di esaminare la bozza di norme vincolanti d'impresa sino a giungere all'adozione di un testo conforme ai riferiti principi in materia.

Il parere di conformità espresso dalla *lead Autority* è sufficiente – in virtù del principio del mutuo riconoscimento che regola i rapporti tra le Autorità che hanno aderito ad una specifica dichiarazione di intenti – al rilascio delle autorizzazioni nazionali[254] propedeutiche, se previste dai singoli ordinamenti,

[253] V. Gruppo dei Garanti europei *ex* art. 29, 14.04.2005, Documento di lavoro n. 107, doc. *web* n. 1608256, Documento di lavoro con cui si stabilisce una procedura di cooperazione per il rilascio di pareri congiunti in merito alle adeguate garanzie derivanti dalle "Norme d'impresa vincolanti" (*"Binding Corporate Rules"*), reperibile su *www.garanteprivacy.it/web/guest/home /docweb/-/docweb-display/export/1608256*.

[254] Per una ricognizione delle autorizzazioni rilasciate dal Garante della *privacy* relativamente al trasferimento di dati all'estero secondo le modalità fissate nelle BCR, *cfr. www.garante*

al trasferimento aziendale extraeuropeo dei dati personali indicati dalle stesse *Binding corporate rules*.

Il trasferimento dei dati verso Paesi terzi rispetto all'Unione è lecito, oltre che nelle ipotesi già analizzate e soggette a specifica autorizzazione, anche quando ricorrono le circostanze previste dall'art. 43, d.lgs. 196/03. In particolare, si può procedere a tanto se *"a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta; b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato; c) è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21; d) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2; e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla*

---

privacy.it/web/guest/home/ricerca?p_p_id=searchportlet_WAR_labcportlet&p_p_lifecycle=0.

legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale; f) è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia; g) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati"[255].

È evidente che le fattispecie previste dal citato art. 43 non sono rilevanti per le ipotesi di *cloud computing* ad eccezione della possibilità di procedere ad un trasferimento extraeuropeo quando l'interessato ha manifestato il proprio consenso nelle forme previste dalla legge. Tale ultima circostanza, infatti, pur essendo di difficile attuazione, potrebbe verificarsi nelle dinamiche del *cloud computing* se l'utente *cloud* titolare del trattamento, al momento dell'instaurazione del rapporto con i singoli interessati, acquisisce la loro espressa autorizzazione.

[255] Così art. 43, co. 1, lett. a - g, d.lgs. 196/03.

Il Reg. UE 2016/679 ha sostanzialmente ripreso l'impostazione data dalla Direttiva 95/46/CE al tema del trasferimento dei dati personali verso Paesi terzi. Quest'ultimo, infatti, è consentito, senza la necessità di autorizzazioni specifiche, se lo Stato di destinazione garantisce un livello di protezione adeguata[256] che sarà valutato, ancora una volta, dalla Commissione Europea[257]. L'applicazione della disciplina regolamentare è stata estesa anche alle ipotesi di trasferimento di dati alle Organizzazioni internazionali[258].

In assenza della predetta decisione di adeguatezza, il trasferimento può comunque avvenire se lo Stato extraeuropeo o l'Organizzazione internazionale riconoscono agli interessati adeguate garanzie e strumenti di ricorso effettivi per far valere i propri diritti.

[256] V. art. 45, Reg. UE 679/2016.

[257] La Commissione, nel valutare l'adeguatezza del livello di protezione, prende in considerazione, ai sensi dell'art. 45, co. 2, i seguenti elementi: *"a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento; b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali"*.

[258] *Cfr.* Reg. UE 679/2016, capo V.

Le clausole contrattuali tipo adottate dalla Commissione e le norme vincolanti d'impresa[259] sono considerate, nuovamente, "garanzie adeguate" insieme alle altre fattispecie introdotte dall'art. 46, Reg. UE 2016/679[260].

È importante rilevare che le autorizzazioni rilasciate, ai sensi dell'art. 26, co. 2, Direttiva 95/46/CE, da uno Stato membro o dall'Autorità di controllo competente, resteranno valide fino a quando non saranno modificate, sostituite o abrogate, dalla stessa Autorità di controllo; le decisioni adottate dalla Commissione in base all'art. 26, co. 4, Direttiva 95/46/CE, invece, resteranno valide se non modificate, sostituite o abrogate, da una decisione adottata ai sensi dell'art. 46, co. 2, Reg. UE 2016/679[261].

Il Reg. UE 2016/679, infine, ha previsto, in linea con la disciplina oggi ancora vigente, alcune ipotesi in cui è possibile effettuare il trasferimento *extra*

---

[259] Il Regolamento *privacy* ha previsto una specifica disciplina per le norme vincolanti d'impresa che oggi, come anticipato, sono adottate sulla base dello schema elaborato dal Gruppo dei Garanti europei ex art. 29. Sul punto v. art. 47, Reg. UE 2016/679.

[260] L'art. 46, co. 2 e 3, Reg. UE ha ampliato il novero degli altri trasferimento consentiti prevedendo che *"2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo: a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici; b) le norme vincolanti d'impresa in conformità dell'articolo 47; c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o*

f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

3. Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1: a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati".

[261] *Cfr.* art. 46, co. 5, Reg. UE 2016/679.

UE, con le modalità di cui all'art. 49, anche in assenza di una decisione di adeguatezza *ex* art. 45, co. 3, o di adeguate garanzie ai sensi dell'art. 46.

Perché ciò accada è necessario che *"a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato; d) il trasferimento sia necessario per importanti motivi di interesse pubblico; e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri"*[262].

[262] Così art. 49, co. 1, lett. a - g, Reg. UE 2016/679.

Capitolo V
La responsabilità extracontrattuale del *cloud provider*

SOMMARIO: 1. La responsabilità dei *provider* ed il modello USA; 2. Le attività dell'*internet service provider* (ISP); 3. Responsabilità dell'ISP per illecito (*ex* art. 2043 c.c.) e responsabilità oggettiva (*ex* art. 2051 c.c.) prima del d.lgs. 70/03; 4. Il d.lgs. 70/03: la responsabilità per colpa specifica; 4.1. Responsabilità nell'attività di semplice trasporto (*Mere conduit*); 4.2. Responsabilità nell'attività di memorizzazione temporanea (*Caching*); 4.3. Responsabilità nell'attività di memorizzazione di informazioni (*Hosting*); 5. (Segue) Assenza di un generale obbligo di sorveglianza; 6. La responsabilità dei *cloud provider*.

1.- *La responsabilità dei provider ed il modello USA.*

Il *cloud provider* rientra a pieno titolo nel novero degli *internet service provider* (ISP) che, nel corso degli anni, hanno assunto un ruolo sempre più nevralgico per il funzionamento della rete.

Per un'analisi più completa dei profili giuridici del *cloud computing*, quindi, è opportuno inquadrare la disciplina relativa all'eventuale responsabilità extracontrattuale del *cloud provider* verificando se i principi sviluppati in via generale per la responsabilità degli ISP ben si adattano ai servizi offerti da questa particolare tipologia di intermediari.

La responsabilità degli ISP ove generalizzata e resa sostanzialmente obiettiva, rischierebbe di minacciare la sopravvivenza degli attuali servizi *internet*. La stessa, tuttavia, non può essere esclusa in ogni caso e a qualsiasi

condizione. Al proposito si deve premettere che la materia è regolata dagli artt. 14, 15, 16 e 17 del d.lgs. 70/03[263] che, recependo le disposizioni della Direttiva 2000/31/CE[264], descrivono gli obblighi di condotta dell'ISP lasciando, però, ampio spazio all'interpretazione giurisprudenziale che, dunque, diventa determinante.

Gli ISP sono diventati, loro malgrado, sempre più spesso protagonisti di contenziosi giudiziari nell'ambito di un contesto tecnologico caratterizzato dal ruolo sempre più attivo degli utenti nella creazione e nella circolazione di contenuti digitali grazie all'avvento del *cd. web* 2.0[265].

Tale circostanza, se da un lato ha favorito la libertà di manifestazione del pensiero, lo sviluppo economico e l'interazione sociale, dall'altro ha determinato il rischio di illeciti connessi alle violazioni di altrui diritti quali, a titolo esemplificativo, quello alla *privacy*, all'identità personale, alla reputazione, al decoro ed alla proprietà intellettuale.

La difficoltà di individuare l'autore dell'illecito e la volontà di bloccare i relativi effetti dannosi, spingono il titolare del diritto leso ad agire anche nei confronti dell'intermediario. È necessario, quindi, provare a chiarire quando, in presenza di illeciti compiuti dai fruitori dei servizi offerti, è possibile imputare una responsabilità all'ISP e quando, di contro, è possibile escluderla.

---

[263] D.lgs. 09.04.03, n. 70, Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.

[264] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), reperibile su *http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32000L 0031&from=IT*.

[265] Con tale termine, a partire dalla fine del 2004, anno della "*Web 2.0 conference di O'Reilly Media*", si indica il nuovo *world wide web* (*www*) caratterizzato da un'elevata interazione tra l'utente ed il sito *web* (e.g. *google+*, *facebook*, i *forum* ed i *blog* in generale, *etc.*) rispetto alla staticità del passato.

Prima di analizzare le soluzioni fornite dal nostro ordinamento sulla scorta delle previsioni comunitarie, è opportuno accennare, anche in ragione della natura transnazionale del fenomeno *cloud*, al modello statunitense precursore e probabile fonte di ispirazione della Direttiva sul commercio elettronico.

Il sistema USA distingue tre ipotesi di responsabilità: la *direct liability*, la *contributory liability* e la *vicarious liability* corrispondenti, rispettivamente, alla responsabilità diretta, a titolo di concorso ed a titolo di vigilanza o per fatto altrui di cui agli artt. 2043, 2055 e 2049 c.c.

In particolare, si parla di responsabilità diretta quando l'illecito è riconducibile allo stesso *provider*, di responsabilità a titolo di concorso se il *provider* ha contribuito all'illecito restando inerte pur avendone conoscenza ovvero coprendo l'anonimato del reale responsabile e, infine, di responsabilità per fatto altrui quando il *provider* non ha adempiuto, dolosamente o colposamente, ad un obbligo di vigilanza gravante su di lui.

La giurisprudenza statunitense ha posto tali principi alla base delle sue decisioni in materia di responsabilità degli ISP[266] sino all'emanazione di importanti provvedimenti normativi tesi a limitare e circoscrivere la responsabilità degli stessi intermediari anche rispetto al tentativo di assimilarla a quella dell'editore[267].

---

[266] Tra le controversie più significative *cfr.* United States District Court, S.D. New York Oct. 29, 1991, No. 90 Civ. 6571, *Cubby* v. *CompuServe* Inc, reperibile su *http://epic.org /free_speech/cubby_v_compuserve.html*; United States District Court, M.D. Florida, Dec. 9, 1993, No. 93-489-Civ-J-20, *Playboy Enterprises, Inc.,* v. *George Frena*, reperibile su *www.loundy.com/CASES/Playboy_v_Frena.html*; United States District Court, N.D. California. March 28, 1994, No. C 93-4262 CW, *Sega Entertainment, Ltd. v. Maphia*, reperibile su *http://www.loundy.com/CASES/Sega_v_MAPHIA.html*.

[267] V. Supreme Court of New York, Dec. 11, 1995, 1995 WL 805178 (N.Y. Sup.), *Stratton Oakmont, Inc.*, v. *Prodigy Svcs. Co.*, reperibile su *https://cyber.harvard.edu/metaschool/fisher /ISP/ISPc4.html*.

In particolare, il *Communication Decency Act* (CDA) del 1996 ha escluso la responsabilità dei *provider* per l'illiceità dei contenuti pubblicati da terzi; la Corte Suprema USA ha, inoltre, precisato che *"l'immunità prevista dalla section 230 del communication decency act protegge la libertà di espressione su Internet e incoraggia l'autocontrollo dei providers come inteso dal legislatore, ne consegue che non è consentito perseguire civilmente o penalmente gli Internet providers per il materiale postato da terzi, quindi chi si reputa leso nei suoi diritti ovvero nella sua onorabilità deve citare in giudizio la fonte originaria della diffamazione"*[268].

Il *Digital Millennium Copyright Act* (DMCA)[269] è, invece, la norma di riferimento in materia di responsabilità degli ISP per gli illeciti derivanti dalla violazione del diritto d'autore ad opera degli utenti *web* che sfruttano i servizi offerti dagli intermediari.

La disposizione prevede, in primo luogo, un'esenzione di responsabilità per i *provider* che si limitano a "trasportare" informazioni e a fornire accesso alla rete[270]. A loro volta, i fornitori di servizi *hosting*[271], quelli di servizi di *caching* ed i gestori di *"local information tools"* non sono responsabili o corresponsabili della violazione del diritto d'autore altrui se non hanno effettiva consapevolezza dell'illecito o di fatti comunque idonei a rendere palese l'antigiuridicità delle condotte poste in essere dai loro clienti. Laddove

[268] Federal jurisdiction [Usa] Supreme court, 20.11.2006, *Barrett* v. *Rosenthal*, in *Foro it.*, Rep. 2007, voce *Diritto comparato* [2250], n. 408.
[269] Per una ricognizione generale del Digital Millennium Copyright Act (DMCA), v. *www.copyright.gov/legislation /dmca.pdf*.
[270] V. DMCA § 512 (a), reperibile su *www.copyright.gov/title17/92chap5.pdf*. Per un più preciso inquadramento dell'attività di mero trasporto delle informazioni *cfr.* il successivo § 2.
[271] Per un più preciso inquadramento di tale attività *cfr.* il successivo § 2.

acquisiscono tale consapevolezza, infatti, devono agire tempestivamente per rimuovere o impedire l'accesso ai contenuti oggetto di contestazione[272].

Il rispetto di queste condotte, utili a beneficiare dell'esenzione di responsabilità, è da coordinare con il meccanismo del *"notice and takedown"* che presuppone una circostanziata *"notification"*, in merito ad un comportamento atto ad integrare una violazione del *copyright*, da cui, come visto, deriva l'obbligo, per il *provider*, di attivarsi[273].

Le segnalazioni di presunte violazioni del diritto d'autore devono essere corredate da un'idonea prova della titolarità del diritto vantato e recare la precisa indicazione del contenuto illecito e dell'indirizzo elettronico presso cui può essere rinvenuto.

Se la segnalazione è completa, l'ISP deve rimuovere il contenuto incriminato informando contestualmente l'utente che ha effettuato il relativo *upload*. Tale soggetto, ricevuto l'avviso, ha la possibilità di opporsi alla cancellazione dimostrando, con una *counter notice*, la legittimità del proprio comportamento.

Il *provider*, a sua volta, se ritiene fondata la *counter notice*, procede al ripristino del materiale in precedenza rimosso continuando a beneficiare, in ogni caso, di un'esenzione di responsabilità. In seguito, il contenuto potrà essere definitivamente cancellato solo in presenza di un provvedimento da parte dell'Autorità giudiziaria.

---

[272] V. DMCA § 512, reperibile su *www.copyright.gov/title17/92chap5.pdf*.
[273] Per un'attenta analisi del *notice and takedown* nell'ambito del *Digital Millennium Copyright Act*, v. F. DELL'AVERSANA, *Le libertà economiche in internet: competition, net neutrality e* copyright, Roma, 2014, p. 204 ss.

2.- ***Le attività dell'internet service provider (ISP).***

Per meglio comprendere la disciplina europea e nazionale in materia di responsabilità degli ISP è opportuno chiarire in che cosa consistono le loro attività a cui devono poi essere ricondotti i servizi offerti dai *cloud provider*; ciò consente di ricostruirne meglio la responsabilità ed individuare i principi cui fare riferimento per disciplinarla.

I principali servizi offerti dagli ISP possono essere così raggruppati e identificati[274]:

a) connettività, accesso e trasporto dati;

b) messa a disposizione di spazio *web* attraverso attività di memorizzazione duratura delle informazioni (*hosting*) e/o memorizzazione temporanea (*caching*);

c) predisposizione e fornitura di contenuti *web* (*content provider*).

Fondamentale per accedere al *cyberspace* è, evidentemente, il servizio di connettività garantito dagli *access provider*[275], tradizionalmente distinti in *access provider* di primo livello, che garantiscono un accesso diretto alla rete, o *access provider* di secondo livello che, invece, consentono un accesso mediato ad *internet*, attraverso il collegamento ad altri *provider*. Nella prima tipologia di *access provider* è possibile, poi, individuare i cd. *network provider*

---

[274] Sulla classificazione funzionale dei servizi *internet*, anche se in un'ottica ormai superata dalla stessa innovazione tecnologica, *cfr.* Corte Suprema degli Stati Uniti, 26 giugno 1997, in *Foro it.*, 1998, IV, 23 e Corte Federale degli Stati Uniti, Distretto Orientale della Pennsylvania, 11 giugno 1996, in *Dir. inf.,* 1996, 606 ss. Oltre ai servizi elencati e più rilevanti ai fini del presente lavoro si considerino i servizi di a) posta elettronica e posta elettronica certificata; b) le *mailing list* ed i *newsgroup*; c) VOIP; d) *chat*; e) videoconferenza; f) *Application Service Provider* (ASP); g) *antivirus* ed *antispamming*; h) registrazione di nomi di domino *etc.*

[275] Sulla diversa terminologia utilizzata per identificare *Provider* che svolgono tale tipo di attività, *cfr.* M. GAMBINI, *Le responsabilità civili dell'*Internet service provider*,* Napoli, 2006, p. 17, nt. 7.

proprietari di importanti infrastrutture di telecomunicazione e, fornitori di banda e connessione agli altri ISP. L'ingresso nel *cyberspace* avviene grazie all'interazione tra il *client* (il PC con cui ci si connette alla rete) ed il *server* dell'*access provider* per il tramite dei *modem* collegati ai PC dell'utilizzatore e del *provider*. La connessione è preceduta dall'autenticazione dell'utilizzatore da parte del fornitore del servizio di accesso. A seguito del riconoscimento dell'utente viene attribuito in automatico, dal sistema del *service provider*, un indirizzo IP[276] dinamico che, individuando univocamente il PC *client* sulla rete, consente al protocollo di trasmissione *internet* di riconoscere le macchine connesse alle rete garantendo lo scambio di dati ed il funzionamento del *web*.

L'*access provider* può fornire ulteriori servizi accessori agli utilizzatori ma, in tal caso, dovrà valutarsi diversamente, rispetto alle previsioni di cui all'art. 14 del d.lgs. 70/03, la sua posizione in merito ad eventuali "responsabilità", considerando il ruolo effettivamente svolto e procedendo, quindi, all'individuazione ed all'imputazione delle attività effettuate *on-line*.

Tipica dei prestatori di servizi della società dell'informazione è l'attività di memorizzazione dei dati che, come anticipato, può essere duratura (*hosting*) o temporanea (*caching*): essa è essenziale per il funzionamento e l'esistenza del *web*.

---

[276] IP: *"sequenza apparente di quattro numeri – in realtà quattro byte – intervallati da un punto (es. 197.234.2.67). Poiché si tratta di quattro byte (un byte è composto da 8 bit) i valori che può assumere ogni "tripletta" sono uguali al numero dei valori che può assumere un bit (cioè due) elevato al numero dei bit presenti nella tripletta stessa (cioè 8): si avrà pertanto $2^8=256$"* così V. STANCA, *I crimini informatici*, Matelica, 2006, p. 22.

Quest'ultimo è caratterizzato da un insieme amplissimo di contenuti multimediali e di servizi accessibili a tutti o ad una parte selezionata[277] di utenti *internet* e costituisce la più grande possibilità offerta a privati, aziende ed enti pubblici di ottenere visibilità in ogni parte del mondo.

Detti contenuti, come è noto, sono organizzati in pagine *web* realizzate con appositi linguaggi di programmazione (quali l'*html*, *dhtml*, *java*, *php*, *xml*, *etc.*). L'insieme di più pagine *web*, correlate tra loro tramite *link* (collegamenti ipertestuali) costituisce un sito *web*, ovvero una struttura ipertestuale di documenti informatici accessibili con un *browser* (come *Internet Explorer*; *Mozilla Fire Fox*; *Safari*; *etc.*) tramite *World Wide Web* (www) su rete *internet*.

Tutti coloro che dispongono di uno spazio di memoria su di un *computer host* collegato alla rete possono, quindi, pubblicare i propri contenuti raccolti in pagine *web* con l'evidente possibilità di diventare "editore" e conseguentemente raggiungere capillarmente un pubblico vastissimo con un esiguo impegno economico. Un sito *web* è raggiungibile, come noto, attraverso la digitazione dell'indirizzo dello stesso, meglio conosciuto come nome di dominio[278] strutturato su tre livelli[279].

---

[277] Si pensi alle pagine *web* caratterizzate da un accesso riservato ai soli titolari delle credenziali di identificazione.

[278] Il *Domain name system* (DNS) corrispondente all'indirizzo IP della macchina su cui è allocato il sito ed utilizzato per semplificare l'attività di ricerca e di reperimento da parte degli utilizzatori che, altrimenti, dovrebbero ricordare, per la fruizione del servizio *web*, sequenze numeriche piuttosto che un nome testuale memorizzabile più facilmente da tutti i fruitori ed in grado di garantire un'ampia diffusione di *internet* anche tra utenti non tecnici. Per una completa analisi delle problematiche tecnico giuridiche sottese al nome di dominio anche nell'ottica dell'omonimia e confusione tra i nomi di dominio, v. M. FARINA, *Diritto e nuove tecnologie*, Forlì, 2007, p. 169 ss.; C.M. CASCIONE, *I* domain names *come oggetto di espropriazione e di garanzia: profili problematici*, in *Dir. informazione e informatica*, 2008, 25; G. CASABURI, Domain names *e segni distintivi: qualche riflessione non ortodossa*, in *Arch. civ.*, 2004, 1369 e in *Dir. ind.*, 2004, 339; R. FERORELLI, Domain names*: natura e disciplina giuridica*, in *Ciberspazio e dir.*, 2001, 365; F. DI CIOMMO, *Dispute sui* domain names*, fatti illeciti compiuti via* Internet *ed inadeguatezza del criterio del* locus commissi

L'*hosting provider* è il fornitore di servizi che si limita a mettere a disposizione di un utilizzatore, in maniera duratura, una parte di *hard disk* del proprio *server* (o dei propri *server*) - di cui, però, resta proprietario - al fine di consentire la pubblicazione e l'*upload* di pagine *web* e contenuti multimediali.

L'*hosting provider*, sempre più spesso, oltre a mettere a disposizione degli utilizzatori spazio *web*, offre loro servizi accessori quali la registrazione del nome di dominio del sito, l'assistenza tecnica, il *backup* automatico ed altre simili attività.

Anche l'attività di *caching* comporta la memorizzazione di dati che, però, in tal caso, è automatica, intermedia e temporanea con riferimento ad informazioni messe a disposizione di terzi al solo scopo di renderne più efficace la successiva trasmissione[280]. Affinché possa concretamente configurarsi tale fattispecie è necessaria la contemporanea sussistenza del requisito della "automaticità" della memorizzazione (è da escludere, quindi, l'intervento di qualsiasi operatore), del suo essere "intermedia" (funzionale al successivo inoltro ad altri utilizzatori) nonché del suo essere "temporanea"

---

delicti, in *Foro it.*, 2001, I, 2033; C. GALLI, *I* domain names *nella giurisprudenza - L'analisi dei problemi - Il testo di settantotto provvedimenti italiani dal 1996 al 2001 - Il repertorio sistematico delle massime*, Milano, 2001; P. SPADA, Domain names *e dominio dei nomi*, in *Riv. dir. civ.*, 2000, I, 713. Per un'analisi della questione in un'ottica comparatistica, con particolare riferimento all'ordinamento spagnolo, v. F. CARBAJO CASCON, *Conflictos entre signos distintivos y nombres de dominio en internet,* Cizur Menor, 2002.

[279] Al primo posto l'acronimo *www*, uguale per tutte le tipologie di dominio; al secondo il *second level domain name*, univoco ed in grado di individuare il nome del soggetto titolare dello stesso e/o l'attività a cui ricondurre le pagine *web* con conseguente elevata capacità distintiva per la quale è prevista un'apposita tutela; al terzo posto, infine, il *top level domain* (TLD) rappresentato da una sigla predeterminata che denota la tipologia di sito (.com; .net; .org, etc.) o lo Stato presso cui è stato registrato il dominio stesso (.it; .fr; .us, etc.) in tal caso si parlerà di *country code* TLD.

[280] *Cfr.* sul punto, art. 15 del d.lgs. 70/03.

(memorizzazione limitata al tempo necessario per il successivo inoltro dell'informazione)[281].

Per comprendere la posizione dell'ISP rispetto al contenuto immesso sul suo *server*, è sempre necessario verificare in concreto se l'attività prestata sia di memorizzazione temporanea o duratura. Infatti, l'eventuale protrarsi dei tempi di permanenza di un'informazione sui *server* di *caching* renderà configurabile, in capo all'intermediario, un'attività di *hosting* con conseguenze giuridiche differenti sotto il profilo degli obblighi di condotta e quindi della responsabilità.

Il *content provider* predispone ed immette in rete il contenuto di un sito *web* per conto di un utilizzatore finale organizzando materiale da lui prodotto o a lui fatto pervenire dal committente ma del quale conosce, o comunque deve conoscere, tipologia e contenuto. Il *content provider* per il ruolo svolto, avendo partecipato alla realizzazione ed all'immissione in rete dei contenuti multimediali, è anche responsabile degli stessi, in via autonoma, quando questi ultimi sono esclusivamente da lui predisposti, unitamente all'utilizzatore anche quando è stesso quest'ultimo a fornire i materiali. Il *provider* dovrà pertanto effettuare un controllo preventivo di legittimità degli stessi poiché, ove ciò non avvenisse o comunque fossero immessi in rete contenuti lesivi di diritti di terzi in violazione delle regole di diligenza professionale, l'ISP sarebbe soggetto ad una responsabilità diretta per fatto proprio, con conseguente applicazione delle disposizioni generali in materia di responsabilità extracontrattuale[282]. Non

[281] Nello stesso senso, *cfr.* M. GAMBINI, *op. cit.*, 279 ss.
[282] In tal senso *cfr.* Trib. Cuneo, 19 ottobre 1999, in *Annali it. dir. autore*, 2000, 809 secondo cui *"l'Internet service provider che offre servizi di hosting è responsabile per le violazioni di*

potrà essere invocato, infatti, in questo caso, l'esenzione dall'obbligo generale di sorveglianza *ex* art. 17 d.lgs. 70/03, applicandosi tale disposizione solo alle fattispecie di cui agli artt. 14 (*mere conduit*), 15 (*caching*) e 16 (*hosting*).

3.- *Responsabilità dell'ISP per illecito (ex art. 2043 c.c.) e responsabilità oggettiva (ex art. 2051 c.c.) prima del d.lgs. 70/03.*

Il d.lgs. 70/03, come anticipato, ha recepito la Direttiva sul commercio elettronico caratterizzata dall'obiettivo di armonizzare il mercato all'interno della Unione Europea[283]. Va notato che le disposizioni comunitarie, poi fatte proprie dal legislatore nazionale, hanno sì ad oggetto la tutela dei destinatari dei servizi *internet* ma, anche, la tutela degli operatori del *web*. Ciò per favorire lo sviluppo e la tenuta del nuovo mercato tecnologico, limitando e precisando le responsabilità degli ISP onde evitare che l'eventuale, indiscriminato

---

diritti d'autore nei siti ospitati sul proprio server solo quando ponga in essere una condotta attiva od omissiva, causalmente correlata al danno, ascrivibile quantomeno a titolo di colpa: come accade ad esempio allorché il provider, a conoscenza dell'illecito, cooperi con l'autore dell'immissione di contenuti protetti per la realizzazione del sito". Sulla responsabilità diretta per fatto proprio degli *internet service provider*, anche per attività diverse rispetto a quelle ascrivibili al *content provider*, v. *infra*.

[283] In tal senso *cfr.* il considerando n. 58 e n. 60 della Direttiva sul commercio elettronico secondo cui *"nonostante la natura globale delle comunicazioni elettroniche, il coordinamento delle misure nazionali di regolamentazione a livello di Unione europea è necessario per evitare la frammentazione del mercato interno e per istituire un idoneo quadro normativo europeo. Tale coordinamento contribuirebbe anche a creare una forte posizione comune di negoziato nelle sedi internazionali"* e ancora, *"per assicurare uno sviluppo senza ostacoli del commercio elettronico, il quadro giuridico deve essere chiaro e semplice, prevedibile e coerente con le regole vigenti a livello internazionale, in modo da non pregiudicare la competitività dell'industria europea e da non ostacolare l'innovazione nel settore"*. Non deve trascurarsi, però, l'altrettanta significativa previsione che, in un'ottica ultraeuropea, esclude l'applicabilità delle disposizioni in tutti i casi in cui è opportuno garantire la coerenza della normativa comunitaria con quella internazionale: *"la presente direttiva non deve applicarsi ai servizi di prestatori stabiliti in un paese terzo. Tuttavia, data la dimensione globale del commercio elettronico, e opportuno garantire la coerenza della normativa comunitaria con quella internazionale. La presente direttiva deve far salvi i risultati delle discussioni sugli aspetti giuridici in corso presso le organizzazioni internazionali (tra le altre, OMC, OCSE, Uncitral)"*.

riconoscimento di responsabilità ad essi imputabili possa determinare una paralisi della rete ovvero provocare un innalzamento dei costi dei servizi.

Prima dell'entrata in vigore del d.lgs. 70/03, l'ISP era considerato responsabile per gli atti posti in essere da un proprio utente, solidalmente con lo stesso, qualora con una condotta colposa o dolosa avesse agevolato e/o determinato il fatto dannoso[284]. Ma dovendosi applicare l'art. 2043 c.c., era eccessivamente gravoso l'onere probatorio per il danneggiato che, per chiamare in causa l'ISP, doveva provare la compartecipazione dell'intermediario nell'illecito. Tale orientamento[285], evidentemente collegato al tradizionale dovere civilistico del *neminem laedere,* ha costituito un "porto sicuro" per gli intermediari di *internet* sino a quando non si è iniziata a diffondere la convinzione che bisognasse imputare, per altre vie, anche al *provider* la responsabilità per le violazioni commesse in rete da un proprio utente. La convinzione muoveva dalla esigenza di garantire "sempre" al danneggiato l'individuazione di un soggetto responsabile nei cui confronti far valere gli interessi al risarcimento.

Dapprima si è tentato di assimilare il *provider* alla figura del responsabile editoriale di una rivista o dell'editore televisivo con la possibilità di applicare la disciplina dei reati a mezzo stampa con il conseguente obbligo, per lo stesso ISP, di verificare la legittimità del materiale pubblicato sul *web* a prescindere

[284] Sulle diverse soluzioni prospettate prima dell'entrata in vigore della direttiva v. E. TOSI, *Le responsabilità civili*, in *AA. VV.*, *I problemi giuridici dell'Internet*, a cura di TOSI, Milano, 1999, 233 ss.
[285] *Cfr.* sul punto la motivazione del Trib. Catania, 29 giugno 2004, in *Foro it.,* 2005, I, 1259.

dalla sua formazione e provenienza. Quindi, in più occasioni[286], si è tentato di riconoscere in capo all'ISP una responsabilità oggettiva collegata all'art. 2050 c.c. L'obiettivo, infatti, era quello di equiparare il *provider* (indipendentemente dall'attività effettivamente svolta) all'esercente attività pericolosa con il conseguente aggravamento dell'onere della prova per lo stesso, chiamato a rispondere del fatto illecito di un qualsiasi utilizzatore del *web*, ove non fosse stato in grado di provare di *«aver adottato tutte le misure idonee ad evitare il danno»*. Tale impostazione non ha tuttavia persuaso perché è evidente che l'attività svolta dal *provider «non appare in sé oggettivamente e intrinsecamente fonte di pericolo»*[287]; essa, del resto, basata sulla configurabilità a carico degli ISP di una responsabilità oggettiva per *culpa in vigilando*, determinerebbe la paralisi della rete.

4.- *Il d.lgs. 70/03: la responsabilità per colpa specifica.*

L'avvento delle nuove tecnologie, la loro capacità di penetrazione nel tessuto sociale nonché l'abbattimento delle distanze geografiche e temporali, hanno fatto emergere l'inadeguatezza dei tradizionali meccanismi della responsabilità aquiliana per la risoluzione delle nuove controversie nella società dei servizi dell'informazione.

Il legislatore italiano, sulla scorta della direttiva comunitaria, ha definito un modello di responsabilità dell'ISP strettamente ancorato al criterio della colpa

[286] A titolo esemplificativo, v. Trib. Monza-Desio (ord.), 14 maggio 2001, in *Corr. giur*., 2001, 1625. Per ulteriori citazioni, v. Trib. Catania, 29 giugno 2004, in *Foro it.*, 2005, I, 1259 con nota di DI CIOMMO.
[287] Trib. Bologna, 26 novembre 2001, in *Dir. Autore,* 2002, 332. Sul punto, *cfr.* la ricostruzione effettuata dal Trib. Catania, 29 giugno 2004, *cit*.

"specifica" per violazione di legge, introducendo nel nostro ordinamento norme specifiche e di dettaglio, in considerazione della particolare fattispecie da regolamentare. Queste definiscono presupposti e limiti della responsabilità del *provider*. La responsabilità dei *providers* è disciplinata considerando l'attività effettivamente svolta e discolpando gli stessi, ogni qual volta prestino semplice attività di intermediazione tecnica senza partecipazione attiva alla commissione dell'illecito. Il presupposto di fondo è che l'ISP, prestando servizi utili per la collettività (non certo attività pericolose), non può essere sottoposto ad una responsabilità oggettiva che di fatto paralizzerebbe, o sicuramente rallenterebbe, lo sviluppo della *new economy* e della *net generation*.

Gli artt. 14, 15 e 16 d.lgs. 70/03, consentono di individuare la responsabilità del ISP in relazione a tre specifiche fattispecie: *mere conduit, caching* e *hosting*. Il modello di responsabilità adottato è basato sul concetto di colpa specifica, e si determina per la violazione di determinati obblighi di condotta.

L'elemento soggettivo della colpa è *in ipsa re* (nel verificarsi della condotta) al pari del dolo che si configura qualora il *provider*, a conoscenza di un illecito, ometta di rimuovere l'elemento dannoso dal sito *web* su cui è pubblicato. Il prestatore intermediario, in definitiva, non dovrà limitarsi a garantire il rispetto del principio del *neminem laedere*, ma dovrà adeguare il proprio comportamento agli obblighi previsti dal legislatore in ragione della sua professionalità.

Secondo parte della dottrina[288], la diligenza professionale richiesta dalla legge al *provider*, configura una responsabilità molto simile a quella (contrattuale) per violazione dei relativi obblighi di correttezza *ex* art. 1175 c.c.

La condotta andrebbe valutata anche alla luce dell'art. 1176 c.c., e trattandosi di una diligenza professionale, «*con riguardo alla natura dell'attività esercitata».* Con la conseguenza che la diligenza professionale diverrà parametro al quale rapportare il comportamento dell'ISP nei confronti di tutti i soggetti terzi con cui entrerà in contatto, a prescindere dall'esistenza di un vincolo contrattuale.

La giurisprudenza ha chiarito che *«l'illecito civile on-line può derivare dalla violazione delle norme a tutela del diritto d'autore, dalla violazione del diritto alla riservatezza o di altri diritti della persona, come l'onore o la reputazione, dalla violazione delle norme a tutela dei marchi, dalla violazione delle norme in materia di concorrenza sleale»*[289].

4.1.- ***Responsabilità nell'attività di semplice trasporto (Mere conduit).*** L'art. 14 del d.lgs. 70/03, nel riproporre le previsioni di cui all'art. 12 della Direttiva 2000/31/CE, disciplina la responsabilità del *provider* che fornisce accesso alla rete di comunicazione o consente il semplice trasporto, sempre su una rete, di informazioni fornite da un destinatario del servizio. Il primo comma esclude la responsabilità del prestatore per l'eventuale contenuto illecito delle informazioni trasmesse, a condizione che lo stesso: *a)* non dia

[288] In argomento, v. C. PERLINGIERI, *Le responsabilità dell'Internet provider,* in *Appunti di diritto dei mezzi di comunicazione*, a cura di DI AMATO, Napoli, 2006, p. 252 ss.
[289] V. Trib. Catania 26 giugno 2004, *cit.* Per una analisi delle singole fattispecie di danno ipotizzabili, v. M. GAMBINI, *op. cit.*, p. 242 ss.

origine alla trasmissione; *b)* non selezioni il destinatario della trasmissione; *c)* non selezioni né modifichi le informazioni trasmesse. La disposizione in analisi non impedisce eventuali rimaneggiamenti di carattere tecnico propedeutici alla trasmissione stessa, purché tale azione non comporti alterazione dell'integrità dell'informazione trasferita.

Il secondo comma dell'art. 14 precisa poi che l'attività di trasmissione e fornitura di accesso di cui al comma 1, è caratterizzata anche dalla memorizzazione automatica, intermedia e transitoria delle informazioni trasmesse, purché questa serva solo alla trasmissione sulla rete di comunicazione e che la sua durata non ecceda il tempo ragionevolmente necessario allo scopo. Tale operazione non altera la qualificazione dell'attività dell'ISP, e quindi la configurazione della sua responsabilità, se lo stesso mantiene una posizione terza. Una memorizzazione delle informazioni trasmesse per un periodo superiore a quello necessario alla trasmissione, da verificarsi evidentemente in concreto, comporterà, di contro, il venir meno del *favor* di cui beneficia il prestatore *mere conduit*, con conseguenti obblighi risarcitori. Il generico riferimento alla durata della memorizzazione che non deve eccedere *"il tempo ragionevolmente necessario a tale scopo"*, è strettamente collegato all'innovazione tecnologica. Le opportunità tecniche, infatti, avranno un'implicazione giuridica o meglio determineranno la conseguenza giuridica dettando, nel caso di specie, *"il tempo ragionevole"*, confine tra la posizione neutrale dell'ISP e la sua *"intrusione"* nella trasmissione delle informazioni. In altre parole, sarà la tecnologia e non la

norma a dettare i "tempi necessari" con conseguente assenza di certezza giuridica.

L'art. 14 del d.lgs. 70/03 pone, infine, in capo all'*access provider*, obblighi di intervento a seguito di una richiesta, anche cautelare, da parte dell'autorità giudiziaria o di quella amministrativa competente per materia. Tale previsione, da collegarsi a quella di cui all'art. 17 dello stesso decreto[290], recepisce una mera facoltà lasciata dalla direttiva comunitaria[291] alla discrezionalità degli Stati membri, di prevedere un'autorità con poteri di inibizione rispetto ad un comportamento illecito. Il d.lgs. 70/03 attribuisce i predetti poteri, oltre che all'Autorità giudiziaria, anche alla Autorità amministrativa *"avente funzioni di vigilanza"*. Tale ultimo soggetto può essere individuato, alternativamente ed a seconda dei casi e degli illeciti, nell'Autorità per le garanzie nelle comunicazioni, nel Garante per la protezione dei dati personali oppure nell'Autorità garante della concorrenza e del mercato.

4.2.- *Responsabilità nell'attività di memorizzazione temporanea (Caching).*

L'art. 15 del d.lgs. 70/03, nel riproporre le previsioni di cui all'art. 13 della Direttiva 2000/31/CE, disciplina la responsabilità del *provider* che svolge attività di memorizzazione automatica, intermedia e temporanea di informazioni messe a disposizione di terzi, al *«solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta*. Anche per

[290] *Cfr.* il successivo § 5.
[291] Direttiva 2000/31/CE art. 12, comma 3 *"Il presente articolo lascia impregiudicata la possibilità, secondo gli ordinamenti degli Stati membri, che un organo giurisdizionale o un'autorità amministrativa esiga che il prestatore impedisca o ponga fine ad una violazione"*.

questi intermediari agisce l'esenzione dalla responsabilità a condizione che "*a) non modifichi le informazioni; b) si conformi alle condizioni di accesso alle informazioni; c) si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore; d) non interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni"*. Di particolare interesse è un'ulteriore condizione e cioè che l'ISP "*e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione"*.

È opportuno chiarire subito la differenza tra l'attività di memorizzazione effettuata dal *caching provider* e quella di cui all'art. 14 già analizzata e relativa al prestatore *mere conduit*. Mentre in quest'ultimo caso si fa riferimento ad una "memorizzazione automatica, intermedia e *transitoria*", con riferimento all'attività di *caching* si parla di "memorizzazione automatica, intermedia e *temporanea*". La terminologia utilizzata ed in particolare il riferimento alla *transitorietà* ed alla *temporaneità* consente di individuare nel maggior lasso di tempo espresso dal concetto di temporaneità rispetto a quello di transitorietà, un sicuro elemento distintivo.

Per il *provider* che esercita attività di *caching* è previsto un *favor legis* più limitato rispetto a quello garantito per l'attività di *mere conduit*; le condizioni

imposte dall'art. 15 per godere dell'esonero di responsabilità nei confronti dei terzi, infatti, risultano più gravose. Senz'altro, il *provider* dovrà mantenere una posizione neutrale rispetto alle informazioni memorizzate, omettendo la modificazione delle stesse e qualsiasi interferenza tecnica. Ma dovrà inoltre procedere tempestivamente ad eliminare o disabilitare l'accesso alle informazioni memorizzate, non appena viene a conoscenza del fatto che le informazioni sono illecite, sia su impulso di chi le ha immesse sia di un organo giurisdizionale o amministrativo. È evidentemente rimesso al giudice non solo di accertare se le informazioni sono state memorizzate *temporaneamente*, configurando così l'attività di *caching* in luogo di quella di *mere conduit* o di *hosting*, ma anche di valutare la tempestività dell'intervento di rimozione, onde poter fare discendere il peculiare regime di responsabilità previsto per questa attività intermediaria. Va da sé che l'onore probatorio del "tempestivo intervento" graverà sul *provider* che dovrà, quindi, dimostrare di essersi attivato "tempestivamente" secondo il criterio della diligenza professionale.

Altrimenti, si configurerà una responsabilità aquiliana per i danni a terzi[292].

[292] *"L'intermediario di caching, per evitare di essere ritenuto responsabile, ha l'obbligo di vigilare sulla effettiva presenza in rete dei contenuti che ha memorizzato sulle proprie macchine. Cosa diversa sarà poi verificare se questi, per esonerarsi da responsabilità, possa invocare l'impossibilità tecnica di provvedere alla rimozione delle copie di cache realizzate"* così M. GAMBINI, *op. cit.*, p. 286. Si consideri inoltre che secondo R. BOCCHINI, *La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggettivo permanente*, Napoli, 2003, 147 s., la tecnica *cache "produce memorie a ripetizione su tutti i computer del mondo, onde il problema tecnico consiste nell'esigibilità pratica di una condotta che dovrebbe eliminare non una, ma tutte le memorie dell'informazione originaria al fine di evitare che a quella informazione illecita il pubblico possa, comunque, attraverso la ricerca in Internet, indirettamente pervenire"*.

4.3.- ***Responsabilità nell'attività di memorizzazione di informazioni (Hosting).***

L'art. 16 del d.lgs. 70/03, nel riproporre le previsioni di cui all'art. 14 della Direttiva 2000/31/CE, disciplina l'attività dell'*hosting provider* dettando le condizioni in presenza delle quali il prestatore è esente da responsabilità. In particolare, l'ISP non è responsabile delle informazioni memorizzate, a condizione che nella prestazione del servizio: *"a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso"*.

L'attività di *hosting* si caratterizza, quindi, per la memorizzazione a carattere tendenzialmente duraturo. Va rilevata la distinzione effettuata dal legislatore tra responsabilità penale e responsabilità civile. Si potrà configurare anche la responsabilità penale, oltre a quella civile, ove il prestatore sia *"effettivamente a conoscenza"* del fatto che l'attività o l'informazione sia illecita mentre, si incorrerà meramente in responsabilità civile se il prestatore "*sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione"*[293].

[293] In argomento, v. G. M. RICCIO, *La responsabilità civile degli internet providers*, Torino, 2002, p. 206.

Per quanto attiene ai profili risarcitori, è preferibile ritenere che permane in capo al danneggiato l'obbligo di provare la conoscenza da parte del ISP dell'illiceità delle attività compiute sul *web*.

Ai sensi del art. 16, co. 1, lett. b), l'*hosting provider* deve rimuovere o disabilitare l'accesso alle informazioni illegittime, altrimenti assume responsabilità. In particolare, la richiesta di rimozione o disabilitazione[294] dell'accesso, proveniente dall'autorità giudiziaria competente, dovrà essere ottemperata immediatamente. Diversamente è a dirsi nel caso in cui la comunicazione abbia origine da un soggetto diverso (ad esempio l'interessato o un terzo). In questo caso, l'ISP potrà effettuare un controllo preventivo teso ad una valutazione di liceità per poi valutare l'opportunità della rimozione o della disabilitazione. In questi casi, l'ISP gode di esenzione dalla responsabilità.

La comunicazione non proveniente dall'autorità giudiziaria è idonea, in ogni caso, ad integrare la "conoscenza" prevista dall'art. 16, co. 1, lett. a), d.lgs. 70/03. Il *provider*, quindi, per non incorrere in (cor)responsabililità in presenza di un contenuto caratterizzato, quantomeno, da manifesta illiceità, deve rimuovere lo stesso contenuto dalla rete o disabilitarne l'accesso procedendo, inoltre, ad informare le competenti autorità ai sensi dell'art. 17, co. 2, lett. a)[295].

---

[294] Con riferimento al dovere di rimozione o disabilitazione delle informazioni illecite si consideri, nell'ottica di un necessario bilanciamento di interessi contrapposti, il considerando 46 della Direttiva 2000/31/CE secondo cui *"[…] La rimozione delle informazioni o la disabilitazione dell'accesso alle medesime devono essere effettuate nel rispetto del principio della libertà di espressione e delle procedure all'uopo previste a livello nazionale […]"*. V. anche M. GAMBINI, *op. cit.*, p. 295, che individua evidenti pericoli negli interventi censori. Gli operatori telematici, con azioni indiscriminate di rimozione *"o, magari, prima ancora, di scelta dei materiali da diffondere in rete, potrebbero innescare negli autori di contenuti, che ritenessero di essere stati lesi nel loro diritto costituzionale alla libera manifestazione del pensiero"* forti reazioni anche sotto il profilo della responsabilità contrattuale a carico dei prestatori *"per i danni subiti in conseguenza di rimozioni o disabilitazioni abusive"*.

[295] V. *infra*.

Non si condivide l'opinione di chi – basandosi sulla considerazione che per configurare la responsabilità dell'*hosting provider* devono ricorrere entrambe le condizioni previste dall'art. 16, co. 1, lett. a) e b), d.lgs. 70/03 – ricollega l'obbligo di rimozione esclusivamente ad un ordine dell'autorità[296].

Si ritiene, infatti, di poter affermare che la disposizione in esame ha introdotto due distinte fattispecie attributive di responsabilità[297]. Tale convinzione è avallata da una semplice considerazione: se il legislatore avesse voluto ricollegare l'obbligo di rimozione esclusivamente ad un ordine dell'autorità non avrebbe alcuna ragione di esistere la previsione che consente di escludere la responsabilità nell'ipotesi in cui l'ISP *"non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione"*.

La fattispecie prevista dall'art. 16, lett. b), d.lgs. 70/03, costituisce, pertanto, un'ipotesi alternativa di attribuzione di responsabilità rispetto a quanto previsto dalla precedente lett. a).

A sostegno dell'obbligo di rimozione, a prescindere dall'ordine dell'autorità[298], si deve ulteriormente considerare che, diversamente argomentando, non ci sarebbe stata alcuna necessità di prevedere l'assenza di un generale obbligo di sorveglianza; infatti, se pur il *provider* si attivasse non

---

[296] V., in tal senso, L. BUGIOLACCHI, *La responsabilità dell'host provider alla luce del d.lgs. 70/03: esegesi di una disciplina "dimezzata"*, in *Resp. civ. e prev.*, 2005, p. 195 ss.

[297] Sul punto v. G. CASSANO, P. CIMINO, *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico"*, in *Contratti*, 2004, p. 91 ss.

[298] Sulla necessità di un intervento dell'ISP successivamente alla segnalazione di una violazione anche da parte di soggetto diverso dall'autorità competente, v., *ex multis*, Trib. Napoli Nord 10.08.16, in *Foro it.*, *Archivio merito ed extra*, 2016.1952 e da ultimo Trib. Napoli Nord 03.11.16 e la giurisprudenza ivi citata, in corso di pubblicazione sulla medesima banca dati.

potrebbe eliminare o bloccare il contenuto illecito in assenza di uno specifico ordine in tal senso.

Nella stessa ottica, inoltre, assume particolare rilievo il considerando 46 della Direttiva 2000/31/CE secondo cui l'ISP, per godere di una limitazione di responsabilità, *"[...] deve agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso alle medesime non appena sia informato o si renda conto delle attività illecite [...]"*.

L'esenzione di responsabilità prevista dall'art. 16, co. 1, lett. a) e b), invece, non si applica *"se il destinatario del servizio agisce sotto l'autorità ed il controllo del prestatore"*[299]. L'*hosting provider*, infatti, risponderà per fatto altrui *ex* art. 2049 c.c., in concorso con l'autore dell'illecito, in tutti i casi in cui quest'ultimo, agendo sotto il controllo e/o supervisione dell'organizzazione aziendale dell'*hosting provider*, pone in essere azioni lesive del diritto dei terzi.

5.- *(Segue) Assenza di un generale obbligo di sorveglianza.*

Principio cardine in materia di responsabilità dell'ISP, espressione di una precisa volontà del legislatore comunitario di escludere qualsiasi forma di responsabilità oggettiva per i *provider* per gli illeciti telematici commessi dai loro utenti, è l'esenzione dall'obbligo generale di sorveglianza sui contenuti dei siti *web* che il *provider* stesso non ha formato o concorso a formare. L'art. 17 del d.lgs. 70/03, in conformità dell'art. 15 Direttiva 2000/31/CE, prevede che il *provider*, nelle prestazioni dei servizi di mero trasporto *(mere conduit)* (art. 14), *caching* (art. 15) ed *hosting* (art. 16) *«non è assoggettato ad un obbligo*

[299] V. art. 16, co. 2, d.lgs. 70/03.

generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite»[300].

L'esenzione ha principalmente fondamento pratico, ma può spiegarsi anche come bilanciamento di più interessi giuridici contrapposti. Sotto il primo profilo, sarebbe irragionevole non considerare la quantità di informazioni immesse e fatte circolare in rete per il tramite degli ISP, nonché le continue modifiche apportate dagli stessi utenti ai contenuti *on-line*. Un controllo capillare da parte dei *provider*, a parità di velocità nell'accesso e nella diffusione delle informazioni, sarebbe impraticabile. Se lo si imponesse occorrerebbe prefigurare una notevole riduzione dell'offerta in *internet* e probabilmente una caduta di interesse per la stessa rete. Ma non ci sarebbe d'altronde alcuna garanzia sulla efficacia dei controlli, visto che buona parte degli illeciti che si perpetrano in *internet* non sono riconoscibili a prima vista, né con meccanismi automatici di controllo (*cd.* filtri), né con l'intervento umano[301]: così per le violazioni del diritto d'autore, per il diritto all'altrui immagine, per alcune privative industriali. Anche per le offese al decoro, alla dignità e alla reputazione il controllo non potrebbe prevenire tutti gli illeciti, ma solo quelli plateali. Occorrerebbe anche ammettere che l'ISP abbia diritto di accesso indiscriminato a tutte le informazioni presenti in rete. Ma ciò

[300] Sul punto, v. anche il considerando n. 15 della dir. 2000/31/CE: *"La riservatezza delle comunicazioni è assicurata dall'articolo 5 della direttiva 97/66/CE. In base a tale direttiva, gli Stati membri devono vietare qualsiasi forma di intercettazione o di sorveglianza non legalmente autorizzata di tali comunicazioni da parte di chi non sia il mittente o il destinatario"*.

[301] Sul punto, v. F. DI CIOMMO, *Programmi-filtro e criteri di imputazione/esonero della responsabilità on-line. A proposito della sentenza sul caso Google/Vivi Down*, in *Dir. informazione e informatica*, 2010, 829 ss.

contrasterebbe non solo con l'attuale disciplina a tutela della *privacy*, bensì anche con i principi costituzionali in materia di libertà e segretezza della corrispondenza, nonché di libera manifestazione del pensiero. Sicché, forme di controllo invasive sui materiali circolanti in rete potrebbero incontrare un limite proprio nei principi indicati.

Il legislatore italiano, con l'art. 17, co. 2, d.lgs. 70/03, ha dato attuazione ad una facoltà lasciata agli Stati membri dalla Direttiva sul commercio elettronico[302], prevedendo che il prestatore è comunque tenuto: *"a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite"*.

Con riferimento alla lettera *a*), è da ritenersi che il *provider* debba attivarsi, se informato di una attività illecita presuntamente posta in essere da un utente del *web*, per verificare la veridicità della notizia ricevuta[303]. Solo successivamente, ed in caso di esito positivo della verifica, dovrà informare le autorità competenti e ottemperare alle loro richieste. In particolare, la lettera *b*)

---

[302] *Cfr.* art. 15, co. 2, Dir. 2000/31/CE *"gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati"*.

[303] L'eventuale negligenza del ISP, durante l'attività di verifica, lascia ipotizzare l'instaurazione di procedimenti giudiziari a suo carico.

impone al *provider* di fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione dell'utente. Al riguardo si pone un complesso problema cui il legislatore dovrà mettere mano nel prossimo futuro. L'obbligo di fornire le informazioni in possesso dell'ISP per permettere l'identificazione dell'utente non risolve di per sé il problema dell'anonimato su *internet*. Problema tecnico, anzitutto, ma ovviamente anche problema giuridico che merita un qualche accenno in questa sede.

L'assegnazione ad ogni "macchina" connessa in rete di un indirizzo IP, consente di individuare le linee telefoniche e gli abbonamenti *internet* adoperati durante le connessioni effettuate anche per commettere gli illeciti.

L'indirizzo IP tuttavia non può essere considerato elemento risolutore nell'individuazione dei soggetti che pongono in essere illeciti *on-line*. Invero, l'IP può cambiare con grande facilità, può essere condiviso, occultato[304] e persino falsificato, con conseguente difficoltà se non impossibilità nell'individuazione dell'utente autore dell'illecito. L'IP del resto individua una "macchina" e l'utilizzo di una rete, ma non necessariamente una persona. Non si può dunque meccanicamente imputare l'illecito al titolare della linea con la quale è effettuato il collegamento ad *internet* o a colui che ha stipulato il contratto con l'*access provider* (soggetti che possono anche divergere).

Dunque, all'ISP compete senza dubbio fornire alle autorità tutto il supporto necessario per favorire l'espletamento di attività di indagine tesa ad individuare

[304] Si considerino, ad esempio, i *software* cd. *anonymizer* che svolgendo una funzione di filtro impediscono che resti traccia dell'utente del *file .log* dei siti visitati consentendo la navigazione in incognito.

i soggetti responsabili di un illecito telematico. Ma non può essere chiesto all'ISP di svolgere indagini definitive sotto questo profilo. Spetta alle forze di polizia, agli esperti e ai consulenti nel settore dell'ICT, applicando le *cd. "best practices"* per la corretta acquisizione delle evidenze digitali, individuare, se possibile, le persone responsabili degli illeciti. Non potrebbe, dunque, condividersi, soprattutto se si tratti di responsabilità penale, un orientamento tendente a configurare automaticamente una responsabilità dell'ISP, in tutti i casi in cui lo stesso non sia in grado di fornire alle autorità preposte le informazioni utili per risalire al singolo utente.

Al riguardo non può non farsi riferimento a quanto ha avuto modo di precisare la giurisprudenza di merito[305] in relazione al problema dell'identificazione degli utenti che si rendono autori di illeciti in materia di diritto d'autore. Decisivo è stato l'intervento in giudizio del Garante per la protezione dei dati personali[306], secondo cui la compressione dei diritti fondamentali alla riservatezza e segretezza delle comunicazioni non può non essere considerata, ed anzi deve ritenersi consentita nel rispetto del principio di proporzionalità *"solo in relazione alla salvaguardia di beni giuridici di superiore valore tutelati dalla normativa penale"*. Tale orientamento ha di fatto escluso che l'ISP dovesse fornire al titolare del diritto d'autore le generalità complete dei propri clienti, associate agli indirizzi IP dei *computer*

[305] Trib. Roma, 22 novembre 2007, (ord.), in *Foro it.*, 2008, I, 1329 con nota di E. TUCCI.

[306] *"Posto che, alla luce della disciplina comunitaria, la tutela delle persone fisiche, con riguardo al trattamento dei dati personali, è prevalente rispetto alle esigenze probatorie di un giudizio civile teso all'accertamento della lesione del diritto di sfruttamento economico del diritto d'autore, deve escludersi l'applicabilità dell'art. 156 bis, l. 633/41, in tema di identificazioni dei soggetti implicati nell'illecito, e dell'art. 24 d.lgs. 196/03 al trattamento dei dati personali relativi alle comunicazioni elettroniche e telematiche tra privati, per finalità connesse alla tutela dei diritti soggettivi dei privati"*.

da cui, utilizzando *software* di *file sharing*, sono stati messi a disposizione brani musicali violando il proprio diritto di privativa[307].

Finché il legislatore non disciplinerà l'anonimato in *internet*, stabilendo quali informazioni devono essere assunte dall'*access provider*, come egli le debba trattare e a quali condizioni le debba mettere a disposizione di terzi o delle autorità competenti, sarà certamente molto complesso potere individuare una responsabilità degli intermediari.

6.- *La responsabilità dei cloud provider.*

Inquadrato sotto un profilo generale il tema della responsabilità degli ISP, categoria a cui sono ricondotti i *cloud provider*, è necessario soffermarsi su alcune specifiche funzionalità offerte da questi ultimi per comprendere il loro ruolo nella circolazione di eventuali contenuti illeciti verificando, al contempo, le specifiche condotte a cui sono tenuti per non incorrere in responsabilità.

Questa ricognizione può prendere le mosse dai servizi di *streaming* basati su tecnologia *cloud* che consente da un lato l'*upload* e lo *storage* nel *public cloud*

[307] Nello stesso senso, in un'ottica comparatistica, *cfr.* la pronuncia della Corte giustizia CE, causa C-275/06, in *http//curia.europa.eu* che – chiamata a pronunciarsi su una questione pregiudiziale sorta nell'ambito di una controversia avente ad oggetto il rifiuto da parte di *Telefonica de España* di rivelare alla *Promusicae* (associazione di produttori ed editori musicali ed audiovisivi) l'identità e l'indirizzo fisico di utenti, individuati tramite "indirizzo IP", ritenuti responsabili dello scambio, grazie al sistema *peer to peer*, di archivi contenenti fonogrammi in violazione dei diritti di proprietà intellettuale – ha affermato che la disciplina comunitaria non impone agli Stati membri, in una situazione come quella oggetto della causa principale, di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile. Il legislatore europeo, però, richiede che i singoli Stati, in occasione della trasposizione delle direttive in argomento, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. In sede di attuazione delle misure di recepimento delle dette direttive, poi, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i diritti fondamentali o con gli altri principi generali del diritto comunitario qual è, ad esempio, il principio di proporzionalità.

di contenuti multimediali, dall'altro l'accesso agli stessi contenuti, in modo libero o a seguito di registrazione e *log in*, a tutti i fruitori del *web*[308].

L'*upload* e lo *storage* sul *cloud* pubblico può avvenire anche mediante i cd. *"one click hosting service"* noti anche come *cyberlocker*; in tal caso il contenuto caricato dall'utente, professionale o non, può essere raggiunto solo tramite un apposito *link*, generato automaticamente dal sistema al termine della procedura, che costituisce l'unico strumento per reperire il contenuto in rete.

A differenza dello *streaming* che consente un accesso generalizzato per il tramite di una semplice ricerca per parola chiave, i *cyberlocker* permettono un accesso circoscritto ai soli detentori del *link* che circola, tra i potenziali utenti, secondo le modalità individuate da chi ha immesso i *file* in *cloud*[309].

Il *cloud provider* può riservare ai propri utenti porzioni del proprio sistema *cloud* determinando, così, il fenomeno dell'*individual public cloud*. In altre parole, ogni utente ha a propria disposizione uno spazio "dedicato" per gestire ed archiviare i propri contenuti ed a cui potrà accedere all'occorrenza.

Il *cloud provider* può gestire questo servizio sia consentendo uno *storage* indiscriminato, senza alcun intervento sui contenuti caricati, sia operando una razionalizzazione dello spazio sul *server* attraverso la cancellazione di duplicati del medesimo *file* caricati da altri utenti ed individuati dal sistema tramite il

[308] A titolo esemplificativo si considerino i servizi offerti da *Youtube* (*www.youtube.com*) e da *Spotity* (*www.spotify.com/it*). Nel primo caso gli utenti possono fruire dei contenuti digitali tramite un accesso libero, nel secondo caso, invece, il servizio pur essendo gratuito (almeno nella sua versione *free*) presuppone una registrazione ed un *log in*.

[309] Il *link*, ad esempio, può essere pubblicato su di una pagina *web* o su un *social network*, inoltrato con *email* o classificato ed inserito su siti *internet* dedicati all'indicizzazione per la successiva circolazione dei contenuti reperibili con l'utilizzo dello stesso *link*.

calcolo del relativo *hash*[310] (*cd. single storage*). Tipico è l'esempio dell'*upload* di un identico *file* musicale da parte di utenti diversi; il sistema, verificando la corrispondenza tra i rispettivi *hash*, procederà ad eliminare i duplicati garantendo, in ogni caso, ad ogni singolo utente, la fruizione del contenuto caricato.

L'offerta di servizi di *individual public cloud* può prevedere anche la possibilità per l'utente di condividere *file* e cartelle realizzando una nuova modalità di scambio di contenuti[311].

In considerazione delle delineate funzionalità e con particolare riferimento ai servizi di *streaming* ed ai *one click hosting service*, si può affermare che il regime di responsabilità extracontrattuale del *cloud provider*, in caso di comportamenti illeciti posti in essere dagli utenti, deve essere delineato in termini analoghi a quanto previsto per il fornitore di servizi di *hosting*. Il *provider*, quindi, se non procede a rimuovere i contenuti illeciti di cui è a conoscenza con le modalità previste dalla legge e in generale, se non si adegua alle disposizioni che gli consentono di beneficiare dell'esenzione di responsabilità offerta dall'ordinamento, sarà responsabile per il materiale presente sul *server* da lui gestito e messo a disposizione dell'utente.

---

[310] L'*hash* – come previsto dall'art. 1, co. 1, lett. g, d.P.C.M. 22 febbraio 2013 recante *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71"* – consiste in una *"funzione matematica che genera, a partire da un'evidenza informatica, un'impronta in modo tale che risulti di fatto impossibile a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti"*. In definitiva, se vi è corrispondenza tra gli *hash* generati partendo da due file distinti, si ha la certezza della loro identità di contenuto.

[311] Si pensi, ad esempio, al servizio *Dropbox* (*www.dropbox.com*) che, oltre a consentire lo *storage* di dati in una porzione di *public cloud* riservata all'utente, permette la condivisione di file e cartelle salvati nello stesso spazio *cloud*. Per maggiori indicazioni sul funzionamento delle cartelle pubbliche di *Dropbox* v. *www.dropbox.com /it/help/16*.

La stessa impostazione è valida per le ipotesi di *individual public cloud*; è importante sottolineare, però, che in presenza di *single storage*, il *cloud provider* potrà procedere ad ottimizzare lo spazio sul *server* con l'eliminazione dei *file* "doppione" solo se, sfruttando gli *hash* dei *file*, è in grado di verificare la liceità della loro provenienza soprattutto rispetto ad eventuali violazioni del diritto d'autore. La cancellazione indiscriminata e l'accesso alla copia *"master"* per la fruizione del contenuto, infatti, può determinare il serio rischio di regolarizzare, erroneamente, la posizione di chi ha acquisito in modo illecito i contenuti digitali con conseguente responsabilità del *provider*.

BIBLIOGRAFIA[312]

A

ALPA G., *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Trattamento dei dati e tutela della persona*, V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH (a cura di), Milano, 1998, 26.

AMBRIOLA V., FLICK C., *Dati nelle nuvole: aspetti giuridici del cloud computing e applicazione alle amministrazioni pubbliche*, reperibile su *www.federalismi.it/nv14/articolo-documento.cfm?artid =22061*.

ARNÒ G., LENSI ORLANDI A., *La tutela della privacy nella rete internet*, Torino, 2002.

ARNOLD U., *New dimensions of outsourcing: a combination of transaction cost economics ande the core competencies concept*, in *European Journal of Purchasing & Supply Management*, 2000, 6.

B

BALLARINO T., *La Convenzione di Roma sulla legge applicabile alle obbligazioni contrattuali entra in vigore*, in *Banca, borsa ecc.,* 1991, I, 649.

BARTOLOMUCCI P., MINERVINI E., *La tutela del consumatore telematico*, in *Manuale di Diritto dell'informatica*, D. VALENTINO (a cura di), Napoli, 2016, 347.

BELISARIO E., *Cloud computing*, *eBook* n. 17, Altalex, 2011.

[312] I titoli delle riviste citate sono stati abbreviati utilizzando come modello l'elenco dei periodici del *Repertorio del Foro italiano*.

BENDANI S., *Software as a Service (Saas): aspetti giuridici e negoziali*, in *www.altalex.com /index.php?idnot=44076*.

BENEDETTELLI M. V., *La legge regolatrice delle obbligazioni contrattuali tra convenzione di Roma e diritto internazionale privato comune*, in *Dir. comm. internaz.,* 1996, 715.

BENUCCI S., *Le prime pronunce in tema di "abuso di dipendenza economica",* in G. Vettori (a cura di), *Concorrenza e Mercato*, Milano, 2005, p. 491.

BERGER K. P., *The Creeping Codification of the New Lex Mercatoria*, Aja, 2010.

BIANCA C. M., *Tutela della privacy (l. 31 dicembre 1996, n. 675): Note introduttive*, in *Nuove leggi civ.*, fasc. 2/3, 1999, 209.

BIN M., *L'equilibrio sinallagmatico nei contratti informatici*, in AA.VV., *I contratti di informatica: profili civilistici, tributari e di bilancio*, a cura di G. ALPA – V. ZENO ZENCOVICH, VII, Milano, 1987, p. 68 ss.

BOCCHINI F., QUADRI E., *Diritto Privato*, V edizione, Torino, 2014.

BOCCHINI F., *Tradizione e attualità nel diritto privato*, Napoli, 2009.

BOCCHINI R., *Il contratto di somministrazione di servizi*, in *I contratti di somministrazione e di distribuzione*, R. BOCCHINI, A. GAMBINO, Torino, 2011, 5.

BOCCHINI R., *La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggettivo permanente*, Napoli, 2003, 147.

BOCCHINI R., *La responsabilità extracontrattuale del provider*, in *Manuale di Diritto dell'informatica*, D. VALENTINO (a cura di), Napoli, 2016, 539.

BOCCHINI R., *Sub art. 1560 c.c.*, in *Dei singoli contratti. Artt. 1548-1654*, D. VALENTINO (a cura di), in *Commentario del Codice civile*, GABRIELLI (diretto da), Torino, 2011, 192.

BOCCHINI R., *Sub art. 1563 c.c.*, in *Dei singoli contratti, Artt. 1548-1654*, D. VALENTINO (a cura di), in *Commentario del Codice civile*, GABRIELLI, (diretto da), Torino, 2011, 221.

BOLDONI P., BOLOGNINI L., FULCO D., PELINO E., *Cloud computing e tutela dei dati personali in Italia. Una sfida d'esempio per l'Europa*, in *Diritto, Economia e Tecnologie della Privacy*, 2011.

BOLOGNINI L., FULCO D., PELINO E., BOLDONI P., *Cloud computing e tutela dei dati personali in Italia. Una sfida d'esempio per l'Europa*, in *Diritto, Economia e Tecnologie della Privacy*, 2011.

BOLOGNINI L., PELINO E., *Servizi di cloud computing e protezione dei dati personali in ambito bancario*, reperibile su *www.vecchioistitutoprivacy.dwb.it /cloud_computing_banche_IIP.pdf*.

BONAZZI E., TRIBERTI C., *Guida ai contratti dell'informatica*, Milano, 1990.

BONOMI A., *Il nuovo diritto internazionale privato dei contratti,* in *Banca, borsa ecc.,* 1992, I, 37.

BORTOLOTTI F., *Drafting and Negotiating International Contract. A practical guide,* Parigi, 2008.

BORTOLOTTI F., *Manuale di diritto commerciale internazionale*, Padova, I, 2009.

BRADSHAW S., MILLARD C., WALDEN I., *Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services*, in *International Journal of Law and Information Technology*, 2011, 187.

BUFFONI L., CARINGELLA F., *Manuale di diritto civile*, VI edizione, Roma, 2016.

BUGIOLACCHI L., *La responsabilità dell'host provider alla luce del d.lgs. 70/03: esegesi di una disciplina "dimezzata"*, in *Resp. civ. e prev.*, 2005, 195.

BUTLER J. M., THEILMANN W., YAHYAPOUR R., WIEDER P., *Service Level Agreements for Cloud Computing*, Springer, 2011.

C

CAGNASCO O., COTTINO G., *Contratti commerciali*, in *Trattato di diritto commerciale*, G. COTTINO (diretto da), Padova, 2000.

CARBAJO CASCON F., *Conflictos entre signos distintivos y nombres de dominio en internet,* Cizur Menor, 2002.

CARBONE S. M., *Autonomia privata e contratti internazionali¸* in *Nuova giur. civ.,* 1992, II, 282.

CARBONE S. M., *Autonomia privata nei rapporti economici internazionali e suoi limiti*, in *Riv. dir. internaz. privato e proc.,* 2007, 891.

CARBONE S. M., LUZZATTO R., *Il contratto internazionale,* Torino, 1994.

CARDARELLI F., *La cooperazione tra imprese nella gestione di risorse informatiche: aspetti giuridici del cd. "outsoursing"*, in *Dir. informazione e informatica*, 1993, 85.

CARINGELLA F., BUFFONI L., *Manuale di diritto civile*, VI edizione, Roma, 2016.

CARRILLO POZO L. F., *El contrato internacional: la prestación característica,* Bologna, 1994.

CASABURI G., Domain names *e segni distintivi: qualche riflessione non ortodossa*, in *Arch. civ.*, 2004, 1369 e in *Dir. ind.*, 2004, 339.

CASCIONE C. M., *I* domain names *come oggetto di espropriazione e di garanzia: profili problematici*, in *Dir. informazione e informatica*, 2008, 25.

CASSANO G., CIMINO P., *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico"*, in *Contratti*, 2004, 91.

CAVE J., STARKEY T., GRAUX H., CREESE S., HOPKINS P., ROBINSON N., VALERI L, *The Cloud: Understanding the Security, Privacy and Trust Challenges*, 2010, reperibile su *http://cordis.europa.eu/fp7/ict/security/docs/ the-cloud-understanding-security-privacy-trust-challenges-2 010_en.pdf*.

CENDON P. (diretto da), *Trattato breve dei nuovi danni*, Padova, 2014.

CIMINO P., CASSANO G., *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello "censore telematico"*, in *Contratti*, 2004, 91.

CLARIZIA R., *Contratti e commercio elettronico*, in *Manuale di informatica giuridica e diritto delle nuove tecnologie*, M. DURANTE, U. PAGALLO, Torino, 2012, 316.

COLANGELO G., *Diritto comparato della proprietà intellettuale*, Bologna, 2011.

COLANGELO G., *L'abuso di dipendenza economica tra disciplina della concorrenza e diritto dei contratti. Un'analisi economica e comparata*, Torino, 2004.

COSTANZO P., *Aspetti evolutivi del regime giuridico di Internet*, in *Dir. informazione e informatica*, 1996, 831.

COTTINO G., CAGNASCO O., *Contratti commerciali*, in *Trattato di diritto commerciale*, G. COTTINO (diretto da), Padova, 2000.

COTTINO G., *Del contratto estimatorio. Della somministrazione*, in *Commentario del codice civile*, A. SCIALOJA, G. BRANCA (a cura di), Bologna, 1970, 128.

CREESE S., HOPKINS P., ROBINSON N., VALERI L., CAVE J., STARKEY T., GRAUX H., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, 2010, reperibile su *http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf*.

CRYSTAL N. M., GIANNONI CRYSTAL F., *Something's got to give: breve comparazione tra l'approccio americano ed europeo al cloud computing, soluzioni pratiche*, in *Cultura e diritti per una formazione giuridica*, Pisa, n. 4, ottobre-dicembre 2014.

D

D'AMBROSIO M., *Cloud computing*, in *Manuale di Diritto dell'informatica*, D. VALENTINO (a cura di), Napoli, 2016, 413.

DAVID R., *Le droit du commerce International,* Parigi, 1987.

DE GIACOMO C., *Diritto, libertà e privacy nel mondo della comunicazione globale. Il contributo della teoria generale del diritto allo studio della normativa sulla tutela dei dati personali*, Milano, 1999.

DE LY F., *International Business Law and "Lex Mercatoria"*, Amsterdam-Londra, 1992.

DE MINICO G., *Internet. Regola e anarchia*, Napoli, 2012.

DE NOVA V., *Introduzione,* in *Fonti e tipi del contratto internazionale*, Milano, 1991.

DE VIVO M. C., *Il contratto ed il cloud computing*, in *Rass. dir. civ.*, 4/2013, 1001.

DELL'AVERSANA F., *Le libertà economiche in* internet: competition, net neutrality *e* copyright, Roma, 2014.

DI CIOMMO F., *Dispute sui* domain names*, fatti illeciti compiuti via* Internet *ed inadeguatezza del criterio del* locus commissi delicti, in *Foro it.*, 2001, I, 2033.

DI CIOMMO F., *Programmi-filtro e criteri di imputazione/esonero della responsabilità on-line*. *A proposito della sentenza sul caso Google/Vivi Down*, in *Dir. informazione e informatica*, 2010, 829.

DI RESTA F. (a cura di), *La tutela dei dati personali nella società dell'informazione*, Torino, 2009.

DRAETTA U., *Il diritto dei contratti internazionali,* vol. I, *La formazione dei contratti*, Padova, 1985; vol. III, *La patologia dei contratti,* Padova, 1988.

DRAETTA U., *Internet e commercio elettronico nel diritto internazionale dei privati*, Milano, 2005.

DRAETTA U., *Internet nel diritto internazionale*, in *Diritto dell'informatica*, F. DELFINI, G. FINOCCHIARO (a cura di), Torino, 2014, 3.

F

F. DELFINI, G. FINOCCHIARO (a cura di), *Diritto dell'informatica*, Torino, 2014.

FABIANO N., *I nuovi paradigmi della rete. Distribueted computing, cloud computing e "computing paradigms": abstract sugli aspetti e i profili giuridici*, in *http://www.diritto.it/docs/27973-i-nuovi-paradigmi-della-rete-distribueted-computing-cloud-computing-e-computing-paradigms-abstract-sugli-aspetti-e-i-profili-giuridici?page=2*.

FARINA M., *Creazione e distribuzione di proprietà intellettuale*, in *I contratti dell'informatica, Aspetti civilistici e fiscali*, A. ATTANASIO, G. BELLAZZI, D. D'AGOSTINI, M. FARINA, Forlì, 2008, 67.

FARINA M., *Diritto e nuove tecnologie*, Forlì, 2007.

FERORELLI R., *Domain names: natura e disciplina giuridica*, in *Ciberspazio e dir.*, 2001, 365.

FINOCCHIARO G., *Diritto di internet*, Bologna, 2008.

FINOCCHIARO G., *I contratti ad oggetto informatico*, Padova, 1993.

FINOCCHIARO G., *Lex mercatoria e commercio elettronico. Il diritto applicabile ai contratti conclusi su* Internet, in *Contratto e impr.*, 2001, 571.

FINOCCHIARO G., *Privacy e protezione dei dati personali, Disciplina e strumenti operativi*, Bologna, 2012, 282.

FLICK C., AMBRIOLA V., *Dati nelle nuvole: aspetti giuridici del cloud computing e applicazione alle amministrazioni pubbliche*, reperibile su *www.federalismi.it /nv14/articolo-documento.cfm?artid =22061*.

FOGGETTI N., *Privacy Protection, applicable Law and Jurisdiction Issues in Cloud Computing: an International and EU prospective*, in *Ciberspazio e dir.*, vol. 15, n. 51 (2/3-2014), 207.

FRIGNANI A., *Il contratto internazionale,* in *Trattato di diritto commerciale e di diritto pubblico dell'economia,* diretto da F. GALGANO, vol. XII, Padova, 1990.

FRIGNANI A., *Il diritto del commercio internazionale. Manuale teorico-pratico per la redazione dei contratti,* Milano, 1990.

FRIGNANI A., TORSELLO M., *Il contratto internazionale. Diritto comparato e prassi commerciali*, Padova, 2010.

FULCO D., PELINO E., BOLDONI P., BOLOGNINI L., *Cloud computing e tutela dei dati personali in Italia. Una sfida d'esempio per l'Europa*, in *Diritto, Economia e Tecnologie della Privacy*, 2011.

G

GALGANO F., *La cultura giuridica italiana di fronte ai problemi informatici*, in G. ALPA, V. ZENO ZENCOVICH, *I contratti d'informatica*, Milano, 1986, 379.

GALGANO F., *Lex mercatoria. Storia del diritto commerciale*, Bologna, 1993.

GALLI C., *I domain names nella giurisprudenza - L'analisi dei problemi - Il testo di settantotto provvedimenti italiani dal 1996 al 2001 - Il repertorio sistematico delle massime*, Milano, 2001.

GAMBINI M., *Le responsabilità civili dell'Internet service provider*, Napoli, 2006.

GAMBINO A.M., STAZI A., *Diritto dell'informatica e della comunicazione*, Torino, 2012.

GIANNATTASIO C., *L'appalto*, Milano, 1977.

GIANNONI CRYSTAL F., CRYSTAL N. M., *Something's got to give: breve comparazione tra l'approccio americano ed europeo al cloud computing, soluzioni pratiche*, in *Cultura e diritti per una formazione giuridica*, Pisa, n. 4, ottobre-dicembre 2014.

GIARDINA V., *L'autonomia delle parti nel commercio internazionale*, in *Fonti e tipi del contratto internazionale* (a cura di DRAETTA e VACCA), Milano, 1991.

GIULIANO M., *La loi d'autonomie: le principe et sa justification théorique*, in *Riv. dir. internaz. privato e proc.,* 1979, 217.

GRANCE T., MELL P., *The NIST Definition of Cloud Computing*, reperibile su *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800145.pdf*

GRAUX H., CREESE S., HOPKINS P., ROBINSON N., VALERI L., CAVE J., STARKEY T., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, 2010, reperibile su *http://cordis.europa.eu/fp7/ict/security/docs /the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf*.

GRIGERA NAON H. A., *Choice of law Problems in International Commercial Arbitration*, Tübingen, 1992.

H

HOOFNAGLE H., *Consumer Protection in Cloud Compunting Services*, in *Consumatori, Diritti e Mercato*, 1/2011, 92.

HOPKINS P., ROBINSON N., VALERI L., CAVE J., STARKEY T., GRAUX H., CREESE S., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, 2010, reperibile su *http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2 010_en.pdf*.

HUNTER M., REDFERN A., *Law and Practice of International Commercial Arbitration*, Londra, 1991.

L

LA ROSA M., *Entra in vigore la Convenzione di Roma del 1980 sulla legge applicabile ai contratti,* in *Giur. comm.,* 1991, I, 842.

LAMETTI D., *Cloud computing: verso il terzo Enclosures Movement?*, in *Riv. critica dir. privato*, 2012, III, 363.

LENSI ORLANDI A., ARNÒ G., *La tutela della privacy nella rete internet*, Torino, 2002.

LEONE S., *La concessione del software tra licenza e locazione*, in G. ALPA, V. ZENO ZENCOVICH, *I contratti d'informatica*, Milano, 1986, 349.

LICATA P., *Privacy, a serio rischio gli accordi UE-USA*, reperibile su *www.corriere-comunicazioni.it/tlc/30225_privacy-a-serio-rischio-gli-accordi-ue-usa.htm*.

LISI A., UNGARO S., *Le 5 W del Cloud Computing*, Lecce, *ebook*, 2014.

LUPOI M. A., *Conflitti transnazionali di giurisdizioni,* II vol., Milano, 2002.

LUZZATTO R., CARBONE S. M., *Il contratto internazionale,* Torino, 1994.

LUZZATTO R., *L'entrata in vigore della Convenzione di Roma del 1980 e il nuovo diritto internazionale privato dei contratti*, in *Dir. comm. internaz.,* 1991, 259.

M

MANTELERO A., *Il contratto per l'erogazione alle imprese di servizi di cloud computing*, in *Contratto e impr.*, 2012, 1218.

MANTELERO A., *Privacy digitale*, *in Manuale di informatica giuridica e diritto delle nuove tecnologie*, M. DURANTE, U. PAGALLO, Torino, 2012, 159.

MANTELERO A., *Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, in *Dir. informazione e informatica*, 2010, 674.

MANTELERO A., *Responsabilità aquiliana per uso della Rete e responsabilità del provider*, in *Diritto dell'informatica*, F. DELFINI, G. FINOCCHIARO (a cura di), Torino, 2014, 785.

MARCHINI R., *Cloud Computing: A Practical Introduction to the Legal Issues*, Londra, 2010.

MARRELLA F., *La nuova lex mercatoria,* Padova, 2003.

MAZZIOTTI DI CELSO A., *Abuso di dipendenza economica*, in *La Subfornitura, Commento alla legge 18 giugno 1998, n. 192*, G. ALPA – A. CLARIZIA, Milano, 1999, 247.

MELL P., GRANCE T., *The NIST Definition of Cloud Computing*, reperibile su *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800145.pdf*

MINERVINI E., BARTOLOMUCCI P., *La tutela del consumatore telematico*, in *Manuale di Diritto dell'informatica*, D. VALENTINO (a cura di), Napoli, 2016, 347.

MONTAGNANI M. L., *Primi orientamenti in materia di responsabilità dei fornitori di servizi cloud per violazione del diritto d'autore in rete*, in *Riv. dir. ind.*, 2014, 3, 177.

MOSCONI F., VITTA E., *Corso di diritto internazionale privato e processuale,* V ed., Torino 1994.

MOSHER R., *Cloud Computing Risks*, 2011, reperibile su *www.experis.us/Website-File-Pile/Articles/Experis/FIN_Cloud-Computing-Risks_071111.pdf*.

MULA D., *Il contratto di archiviazione e gestione da remoto dei documenti informatici. Qualificazione del contratto di cloud service*, in *Ianus*, 2014, n. 2.

MULA D., *Standardizzazione delle clausole contrattuali di somministrazione di servizi cloud e benessere del consumatore*, in *Profili interdisciplinari del commercio elettronico*, C. G. CORVESE, G. GIMIGLIANO (a cura di), Pisa, 2016, 146.

MUSELLA A., *Il contratto di outsourcing del sistema informativo*, in *Dir. informazione e dell'informatica*, 1998, 857.

MUSTILL M., *The New Lex Mercatoria: the First Twenty-Five Years,* in *Liber Amicorum Lord Wilberforce*, Oxford, 1987, p. 149.

N

NOTO LA DIEGA G., *Cloud computing e protezione dei dati nel web 3.0*, 2014, reperibile su *http://giustiziacivile.com/soggetti-e-nuove-tecnologie/approfondimenti/cloud-computing-e-protezione-dei -dati-nel-web-30.*

NOTO LA DIEGA G., *Il Cloud computing. Alla ricerca del diritto perduto nel web 3.0*, in *Europa e dir. privato*, 2014, 2, 577.

O

OPPO G., *Princìpi*, Torino, 2001.

P

PALUMBO S., *Cloud computing opportunità e rischi della nuvola*, in *Dir. ed economia mezzi di comunicazione*, 2014, 1, 43.

PAPA A., *Espressione e diffusione del pensiero di internet*, Torino, 2009.

PARKHILL D.F., *The Challenge of the Computer Utility*, Londra, 1966.

PELINO E., BOLDONI P., BOLOGNINI L., FULCO D., *Cloud computing e tutela dei dati personali in Italia. Una sfida d'esempio per l'Europa*, in *Diritto, Economia e Tecnologie della Privacy*, 2011.

PELINO E., BOLOGNINI L., *Servizi di cloud computing e protezione dei dati personali in ambito bancario*, 2015, reperibile su *www.vecchioistituto-privacy.dwb.it/cloud_computing_banche_IIP.pdf*.

PERLINGIERI C., *Le responsabilità dell'Internet provider,* in *Appunti di diritto dei mezzi di comunicazione*, a cura di DI AMATO, Napoli, 2006, 252.

PICCHIO FORLATI L., *La Convenzione di Roma del 1980 sulla legge applicabile ai contratti nell'ordinamento italiano*, in E. JAYME, L. PICCHIO FORLATI, *Giurisdizione e legge applicabile ai contratti nella CEE,* Padova, 1990, 109.

PINTO V., *L'abuso di dipendenza economica 'fuori dal contratto' tra diritto civile e diritto antitrust*, in *Riv. dir. civ.*, 2000, 394.

PIROZZI F., *Il cloud computing. Lex mercatoria e tutela dei dati*, Milano, 2016.

PITTALIS M., *Outsourcing*, in *Contratto e impr.*, 2000, 1006.

PIZZETTI F., *Uomini e dati - Evoluzione tecnologica e diritto alla riservatezza*, in *Foro it.*, 2011, V, 230.

POCAR F., *L'entrata in vigore della Convenzione di Roma del 1980 sulla legge applicabile ai contratti,* in *Riv. dir. internaz. privato e proc.,* 1991, 249.

PROSPERETTI E., *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema cloud*, in *Trattato di Diritto dell'Internet*, G. CASSANO (a cura di), Padova, 2012, 683.

PROSPERI F., *Il contratto di subfornitura e l'abuso di dipendenza economica. Profili ricostruttivi e sistematici*, Napoli, 2002.

Q

QUADRI E., BOCCHINI F., *Diritto Privato*, V edizione, Torino, 2014.

R

REDFERN A., HUNTER M., *Law and Practice of International Commercial Arbitration*, Londra, 1991.

RICCI A., *L'outsourcing e cloud computing*, in *Diritto dell'informatica*, F. DELFINI, G. FINOCCHIARO (a cura di), Torino, 2014, 664.

RICCIO G. M., *La responsabilità civile degli internet providers*, Torino, 2002, 206.

RIFKIN J., *L'era dell'accesso. La rivoluzione della new economy*, Milano, 2000.

RIZZO G., *La Responsabilità contrattuale nella gestione dei dati nel cloud computing*, in *Diritto Mercato Tecnologia*, 2013, 102.

ROBINSON N., VALERI L., CAVE J., STARKEY T., GRAUX H., CREESE S., HOPKINS P., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, 2010, reperibile su *http://cordis.europa.eu/fp7/ict/security/docs /the-cloud-understanding-security-privacy-trust-challenges-2 010_en.pdf*.

ROPPO V., *Il contratto*, in *Trattato di Diritto Privato*, IUDICA, ZATTI (a cura di), Milano, 2001.

ROPPO V., *Introduzione*, in *Trattato della responsabilità contrattuale*, VISENTINI (a cura di), Padova, 2009.

ROSSELLO C., *Commercio elettronico*, Milano, 2006.

ROSSELLO C., *I contratti dell'informatica nella nuova disciplina del software*, Milano, 1997.

RUBINO D., *Dell'appalto*, in *Commentario del codice civile*, A. SCIALOJA, G. BRANCA (a cura di), Bologna, 1973, 25.

RUBINO D., *L'appalto*, Torino, 1980.

RUBINO SAMMARTANO M., *Appalti di opere e contratti di servizi (in diritto privato)*, Padova, 2006, 734.

S

SARAVALLE A., *Commento all'art. 3*, in *Commentario alla Convenzione di Roma*, in *Nuove leggi civ.*, 1995, 942.

SCHMIDT E., *Don't be against the Internet*, in *The Economist*, reperibile su *www.economist.com/theworldin/businnes/displayStory.cfm?story_id=8133511 &d=2007*.

SISTO G., *Le diverse modalità di distribuzione del software: freeware, shareware e trial version*, in G. CASSANO, *Diritto delle nuove tecnologie e dell'internet*, Milano, 2002, 1058.

SOFFIENTINI M., *Cloud computing e privacy*, in *Dir. e pratica lav.*, 2013, n. 42, 2465.

SPADA P., *Domain names e dominio dei nomi*, in *Riv. dir. civ.*, 2000, I, 713.

STANCA V., *I crimini informatici*, Matelica, 2006.

STARKEY T., GRAUX H., CREESE S., HOPKINS P., ROBINSON N., VALERI L., CAVE J., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, 2010, reperibile su *http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-pri-vacy-trust-challenges-2010_en.pdf*.

STAZI A., *"Marketplace of ideas" e "accesso pluralistico" tra petizioni di principio e ius positum*, in *Dir. informazione e informatica*, 2009, 635.

STAZI A., GAMBINO A.M., *Diritto dell'informatica e della comunicazione*, Torino, 2012.

STOLFI M., *Appalto (contratto di)*, in *Enciclopedia del Diritto*, Milano, 1958.

T

THEILMANN W., YAHYAPOUR R., WIEDER P., BUTLER J. M., *Service Level Agreements for Cloud Computing*, Springer, 2011.

TORSELLO M., FRIGNANI A., *Il contratto internazionale. Diritto comparato e prassi commerciali*, Padova, 2010.

TOSI E., *Il contratto di outsourcing di sistema informatico*, Milano, 2001.

TREVES T., *Art. 57*, in *Riv. dir. internaz. privato e proc.*, 1995, 1178.

TRIBERTI C., BONAZZI E., *Guida ai contratti dell'informatica*, Milano, 1990.

TROIANO G., *Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale: alla ricerca di un equilibrio tra diritti dell'utente e doveri del fornitore*, in *Ciberspazio e dir.*, 2011, 233.

U

UNGARO S., LISI A., *Le 5 W del Cloud Computing*, Lecce, *ebook*, 2014.

V

VALENTINO D., *I contratti di informatizzazione d'azienda*, in *Dir. dell'internet*, 2005, 416.

VALERI L., CAVE J., STARKEY T., GRAUX H., CREESE S., HOPKINS P., ROBINSON N., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, 2010, reperibile su *http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-pri-vacy-trust-challenges-2010_en.pdf*.

VIGGIANO M., *Internet, Informazione, regole e valori costituzionali*, Napoli, 2010.

VITTA E., MOSCONI F., *Corso di diritto internazionale privato e processuale,* V ed., Torino 1994.

W

WIEDER P., BUTLER J. M., THEILMANN W., YAHYAPOUR R., *Service Level Agreements for Cloud Computing*, Springer, 2011.

Y

YAHYAPOUR R., WIEDER P., BUTLER J. M., THEILMANN W., *Service Level Agreements for Cloud Computing*, Springer, 2011.

YOO C., *Cloud Computing: Architectural and Policy Implication*, 2011, reperibile su *http://ssrn.com/abstract=1824580*.

ZINCONE A., *Il contratto di outsourcing: natura, caratteristiche, effetti*, in *Annali it. dir. aut.*, 2002, 379.

Z

ZUDDAS G., *Somministrazione. Concessione di vendita. Franchising, in Trattato di diritto commerciale*, V. BUONOCORE (diretto da), Torino, 2003, 36.

ZICCARDI G., *Informatica giuridica. Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, Milano, 2012.