
# QUADERNI DI DIRITTO MERCATO TECNOLOGIA


**Numero 1**
**Anno III**
**Gennaio/Marzo 2013**

CON CONTRIBUTI DI:

Alessio Baldi, Valeria Falce, Monica La Pietra, Francesca Orazi, Maria Cecilia Paglietti, Giulia Pietropaoli, Annalisa Pistilli, Giuseppe Rizzo.

**ISSN (Online edition): 2239-7442**

# *La responsabilità contrattuale nella gestione dei dati nel cloud computing*

**di**
**Giuseppe Rizzo**

**Abstract**: Le tecnologie di *cloud computing* sono diventate una realtà quotidiana, dall'uso "domestico" sino alle più avanzate applicazioni in campo imprenditoriale. Questa relazione si focalizza su alcuni aspetti della responsabilità contrattuale del *cloud service provider*. Si tratta di argomenti di diritto comune che, però, assumono connotazioni particolari quando vengono applicati a servizi innovativi come quelli di *cloud computing*.
Come tutti i contratti, del resto, anche quelli di *cloud computing* possono incontrare delle difficoltà a causa di eventi imputabili o meno al *cloud service provider* e che possono creare ingenti danni all'utente, soprattutto se si tratta di imprese, con effetti "moltiplicatore" di grave portata.
In contratti di questo tipo, infatti, la relazione tra *cloud service provider* e utenti è tale che in caso si verifichi un inadempimento tecnico qualificabile in termini di continuità di servizio, riservatezza, integrità o sicurezza dei dati, lo stesso si riverbera su una vasta platea di utenti che, a loro volta, potrebbero trovarsi nella condizione di arrecare un disservizio ai propri clienti con un'evidente ricaduta sul business del *cloud service provider* a cui è imputato il danno.
È comprensibile, allora, l'interesse da parte di quest'ultimo di circoscrivere l'ambito della propria responsabilità patrimoniale, mentre l'utente aspira a ottenere livelli di tutela adeguati. Un notevole ostacolo è tuttavia rappresentato dalla enorme sproporzione in termini di forza negoziale fra fornitore (che impone le condizioni) e utente. Solo l'utente *consumer* gode su scala europea, di una serie di tutele inderogabili che, in Italia, si rifanno al Codice del Consumo. L'utente *business* dovrà invece attentamente valutare l'offerta ed i livelli di servizio assicurati dal *provider* (*Service Level Agreement*) sia per assicurarsi di essere in linea con le previsioni legislative sulla *privacy* sia per tutelare adeguatamente le informazioni veicolate sulla nuvola, che sovente assumono un valore economico assai cospicuo e possono quindi accedere, ricorrendo determinata condizioni, al regime di protezione previsto per le informazioni industriali e commerciali riservate, oggetto di diritto assoluto.
*Cloud computing technologies have become a daily reality, from "home" use to the most advanced business applications. This report focuses on some aspects of the contractual responsibility of the cloud service provider.*
*These are very common legal issues that, however, take on particular connotations when applied to such innovative services as cloud computing.*

*Like all contracts, cloud computing contracts may encounter difficulties due to events that may or may not be ascribable to the cloud service provider, capable of creating enormous damage to the users, especially in the case of companies, with far-ranging "multiplying" effects.*
*In fact, in contracts of this kind, the relationship between cloud service provider and users is such that should a technical glitch occur, that may be qualified in terms of service continuity, confidentiality, or data integrity or security, this reverberates over a vast field of users which, in turn, may find themselves in a condition of committing a disservice to their own clients, with a clear impact on the business of the cloud service provider blamed for the damage.*
*One may then comprehend the provider's interest in limiting the field of its own property liability, while the user aims to secure adequate levels of protection. However, a major obstacle is that of the enormously imbalanced bargaining power between the supplier (which imposes the conditions) and the user. Only the consumer enjoys, on a European scale, a series of undeniable mandatory protections that, in Italy, are regulated by Consumer's Code. The business user must, on the other hand, carefully assess the offer and the levels of service guaranteed by the provider (Service Level Agreement), both to ensure being in line with the legislative provisions on privacy, and to suitably protect the information carried on the cloud, which often has quite a considerable economic value and may thus, under certain conditions, rise to the protection regime established for confidential trade and industrial information, which is subject to absolute law.*



## 1. I servizi di *cloud computing* fra norme imperative e contratto.

Il *cloud computing* è un fenomeno tendenzialmente transnazionale.
La stessa tassonomia del *cloud* implica, infatti, un trasferimento di dati dal cliente al fornitore del servizio (e spesso la catena di trasferimento non si

limita solo a quest'ultimo) che – il più delle volte – può essere transfrontaliero.
Due dei primissimi problemi che si pongono all'interprete ed all'operatore del diritto sono quindi quello della legge applicabile e quello della giurisdizione.
La risoluzione di tali quesiti richiede una attenta considerazione, da un lato, della natura e della tipologia dei clienti *cloud* (in particolare di questi ultimi, se qualificabili come "consumatori" ai sensi della disciplina comunitaria e nazionale ovvero operatori professionali), dall'altra della struttura del servizio offerto.
Quanto alla legge applicabile, ci saranno almeno quattro ordinamenti che dovranno essere presi in considerazione e precisamente: quello del cliente; quello del fornitore del servizio *cloud*; quello del luogo in cui i dati sono memorizzati (spesso più d'uno, nei casi di struttura c.d. *multi-tenancy*); quello dei soggetti cui i dati memorizzati ed oggetto di trasferimento si riferiscono [1].
Il conflitto di leggi applicabili – almeno limitatamente all'Unione Europea – può essere risolto mediante il ricorso alla disciplina uniforme prevista per le obbligazioni contrattuali [2] (nel caso in cui il tema del contendere riguardi il rapporto fra il cliente ed il fornitore) ed extracontrattuali [3].
Si tratta, peraltro, di una schematizzazione ampiamente inadeguata, sia in considerazione dell'orizzonte territoriale (ben più vasto dei confini dell'Unione Europea) entro cui agiscono le imprese del settore sia perché la determinazione della legge applicabile dipende in concreto anche dalla materia oggetto di controversia (*privacy* [4]; responsabilità contrattuale o extracontrattuale [5]; diritto penale ed investigazioni internazionali; commercio elettronico [6]; proprietà intellettuale;…). A ciò si aggiunga che – su scala mondiale (che è lo scenario cui, con buona pace di chi vorrebbe mettere limiti alla rete, deve essere considerato quello "naturale" del *cloud computing*) – la materia diviene ancor più dinamica e complessa soprattutto in considerazione dei diversi approcci giuridici al di qua e al di là dell'Atlantico [7].
Non è obiettivo del presente intervento quello di esaminare nel dettaglio le varie sfaccettature del problema delle legge applicabile, ma quanto appena sopra sinteticamente rilevato è senz'altro sufficiente ad introdurre una notazione che regge l'oggetto specifico di questa relazione: il contratto rappresenta il più delle volte lo strumento principe mediante il quale le parti (*cloud provider* e cliente) regolano, nel metodo e nel merito, le questioni astrattamente suscettibili di sfociare in un conflitto (oltre, ovviamente, alle prestazioni oggetto del contratto ed alle modalità con cui devono essere rese).
Il contratto diventa quindi piattaforma di normalizzazione di una disciplina legislativa di certo incompleta (almeno se rapportata alla natura proteiforme del *cloud computing* ed alle innumerevoli implicazioni

connesse al funzionamento dei servizi *cloud*) e di difficile coordinamento. Non solo: un chiaro e dettagliato accordo ha indubbie funzioni di trasparenza poiché – se ben redatto (ed, eventualmente, negoziato) e ben inteso dalle parti – consente all'utilizzatore del servizio di focalizzare l'attenzione sui vantaggi e sui rischi dello stesso, con esatta comprensione della qualità delle prestazioni promesse e delle garanzie relative ai dati trattati, utilizzati e immagazzinati presso i *data center* del *provider* [8].
Occorre tuttavia preliminarmente fare un distinguo tra i casi in cui il cliente sia un consumatore e quelli in cui ad accedere ai servizi *cloud* sia un'impresa o un professionista. Nel caso di contratto *cloud* concluso da un consumatore (italiano o, quantomeno, europeo), infatti, quest'ultimo godrà di una tutela minima ed inderogabile contro clausole inique ed irragionevoli, prestata in Italia dal Codice del Consumo [9] e comunque garantita, a livello europeo, dalle direttive (e dalle leggi nazionali di implementazione delle stesse) che, a partire dalla fine degli anni ottanta, hanno progressivamente contribuito a dar forma al sostrato normativo del Codice stesso [10].
Questa relazione, per oggettivi limiti di tempo ed anche vista la platea di uditori, avrà come oggetto il rapporto c.d. B2B e cioè fra un fornitore di servizi *cloud computing* ed un'impresa o un professionista: si tratta di categorie che, in quanto soggetti privi della tutela minima di legge anzi riferita ed economicamente più esposte ad eventuali *default* del *provider* (si pensi ai profili di responsabilità nei confronti dei propri clienti), dovranno prestare maggiore attenzione al contratto ed, in particolare, alle condizioni che regolano la responsabilità del fornitore del servizio.
Occorre tuttavia segnalare che gli operatori professionali, pur se tipicamente destinatari di una protezione affievolita rispetto ai consumatori, non sono radicalmente privi di una tutela imperativa (e successiva) rispetto alla stipula di clausole particolarmente sbilanciate a favore di una delle parti (solitamente quella dotata di maggiore forza contrattuale).
In Italia esiste, infatti, la disciplina dell'abuso di dipendenza economica; a norma dell'art. 9 della l. 192/98, infatti, la legge definisce come dipendenza economica *"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"*.
Il divieto, originariamente elaborato in materia di subfornitura e poi esteso per giurisprudenza costante a tutti i contratti di cooperazione commerciale [11], colpisce (sanzionandole con la nullità, salvo il diritto al risarcimento del danno della parte che ha subito l'abuso) tutte le condizioni ingiustificatamente gravose cui è sottoposta un'impresa (cliente o fornitrice) che si trova in uno stato di dipendenza economica rispetto ad una impresa committente, la quale ultima è nella concreta facoltà di imporre al *partner* condizioni eccessivamente squilibrate a proprio

vantaggio [12]. La dipendenza economica deve essere valutata *"tenendo conto anche della reale possibilità per la parte che ha subito l'abuso di reperire sul mercato alternative soddisfacenti"*: è questo il criterio essenziale di riferimento nell'applicazione della norma, che crea un addentellato alle concrete dinamiche di mercato [13].
Del resto, l'ambito di tutela destinato agli utenti professionali non deve pensarsi limitato ad una (eccentrica) norma nazionale quale quella appena citata. Ed infatti, sebbene l'art. 9 della legge 192/98 non abbia una diretta e chiara matrice comunitaria, è pur vero che essa è evidente espressione della disciplina europea in materia di libera concorrenza nel mercato. Inoltre la fattispecie non è affatto estranea alla legge ed alla giurisprudenza di molti altri Stati membri dell'Unione, come ad esempio la Francia e la Germania [14]. Giova poi notare che anche nel sistema giuridico britannico le piccole e medie imprese non sono prive di una tutela contro condizioni inique e dall'analisi casistica emergono esempi assolutamente calzanti all'ipotesi di relazioni contrattuali aventi ad oggetto servizi di *cloud computing* [15].
Inoltre, con prospettiva ancor più ampia, principi analoghi a quelli appena rammentati sembrano contenuti nella nuova *lex mercatoria*, ovvero nei "*Principles of International Commercial Contracts*" [16] Unidroit, nel quadro dei quali la disciplina sul contraente debole trova espressione nell'istituto della *Gross Disparity* (art. 3.10) [17].
Tale digressione non sembra davvero inutile nel quadro che andiamo delineando.
È infatti un dato di comune evidenza che i rapporti fra *cloud provider* ed utente sono sovente connotati da una sproporzione di forza contrattuale o comunque da importanti asimmetrie informative e conoscitive, così che non è affatto improbabile che possa presentarsi sin dall'inizio una pericolosa situazione di squilibrio suscettibile di portare, *medio tempore*, ad abusi riconducibili alle norme (o ai principi) sopra rammentati.
L'abuso, peraltro, tende ad assumere rilevanza non solo e non tanto al momento della conclusione del contratto quanto nel corso della sua esecuzione o addirittura al momento della cessazione del rapporto. Ed infatti, applicando l'istituto dell'abuso di dipendenza economica, mi sembra che un eventuale contegno illecito del *service provider* possa assumere rilevanza solo nel momento in cui non esista più una *"reale possibilità per la parte che ha subito l'abuso di reperire sul mercato alternative soddisfacenti"* (il che di solito non accade al momento in cui l'utente sceglie il fornitore, considerata l'offerta assai ampia sul mercato [18]). A tal proposito si rammenta la fattispecie (elaborata dalla dottrina e dalla giurisprudenza tedesca) della c.d. "dipendenza dell'impresa", detta anche "da rapporti commerciali", che si ravvisa nel caso di un rapporto tra impresa in posizione dominante relativa e impresa dipendente nel quadro del quale quest'ultima si trova nell'impossibilità di rivolgersi ad altri senza

sopportare incisive ripercussioni sfavorevoli sulla propria attività. Tale situazione si verifica frequentemente nel caso modifica *in itinere* di rapporti di lunga durata [19] ovvero nel caso di cessazione inopinata ed imprevista del rapporto (per recesso o disdetta del fornitore) quando l'impresa dipendente abbia concentrato la propria attività su di un unico fornitore; in tali circostanze l'impresa dipendente potrebbe aver sopportato investimenti rilevanti e difficilmente recuperabili nel tempo necessario al cambio di fornitore ovvero potrebbe accadere che un cambio di partner commerciale o industriale diventi concretamente impossibile o comunque irragionevolmente costoso. La casistica giurisprudenziale non contempla evidentemente (ancora) contenziosi su servizi di *cloud computing*, ma (per quanto detto sinora) è indubbio che la norma potrebbe trovare applicazione ad ipotesi in cui dovesse verificarsi un *lock in* (assoluto o relativo) [20] a sfavore dell'utente.

## 2. I modelli contrattuali: (molte) facoltà dei *cloud provider* e (poche) garanzie per gli utenti. I *Service Level Agreement*.

La prassi contrattuale che si va formando sembra non priva di aspetti critici (per il cliente). Fra questi meritano particolare attenzione la rigidità degli accordi (c'è la tendenza dei fornitori – soprattutto se colossi del settore – a proporre modelli contrattuali sui quali l'utente non è in grado di esplicare alcuna forza negoziale), la genericità di talune rappresentazioni rilevanti ai fini dell'esatta individuazione delle prestazioni dedotte come oggetto del contratto (definizione delle tecnologie, dislocazione dei *data center*, misure di sicurezza, risorse umane dedicate e loro specializzazione) o la scarsa trasparenza (per lo più sulle garanzie e sulle esclusioni di responsabilità).
E siccome i contratti di servizi *cloud* possono, come tutti i contratti, subire delle alterazioni funzionali dovute all'inadempimento del fornitore del servizio o all'esecuzione negligente o in mala fede, vorrei innanzitutto individuare tre aree principali cui, in siffatta prospettiva, dovrà porsi attenzione nell'esame di un contratto di servizi *cloud* (e ciò tanto che il contraente abbia forza contrattuale sufficiente per negoziare con *cloud service provider* delle condizioni di contratto *tailor made* tanto che debba "subire" le condizioni generali di contratto unilateralmente predisposte dal fornitore).
Le aree critiche sono, a mio avviso, le seguenti:
a) I *Service Level Agreement* (SLA);
b) Le previsioni sulla riservatezza e sicurezza dei dati sotto il profilo della *privacy*;
c) Le previsioni sull'integrità e sicurezza dei dati considerati come beni aziendali (riservati).

I *Service Level Agreement* contribuiscono a definire con precisione l'oggetto del contratto. Nel caso di servizi di *cloud computing* essi riguarderanno parametri tecnici oggettivi e misurabili (ad es. *uptime* e *downtime*, tempi di risposta, tempi di presa in carico del servizio,…) [21]. È noto che in dottrina esiste una difformità di vedute circa l'inquadramento delle obbligazioni del *cloud service provider* come obbligazioni di mezzo o di risultato ed allo specifico argomento è riservata una dettagliata ed relazione pomeridiana. Senza voler quindi in questa sede toccare, se non tangenzialmente, il tema si può tuttavia sostenere senza particolari perplessità che l'obbligazione gravante sul *provider* è quella di eseguire le prestazioni pattuite nel puntuale rispetto dei livelli qualitativi di servizio prestabiliti (e generalmente riportati in allegati tecnici al contratto o, nel caso di contratti elettronici, in documenti che siano espressamente richiamati nel contratto) [22].
Dalla combinazione fra livelli di servizio promessi e regolamentazione della responsabilità per violazioni o incidenti discenderanno i primi fondamentali parametri per definire l'ambito della responsabilità del *cloud service provider* per inadempimento del proprio obbligo di fare.
È stato correttamente osservato [23] che, anche nei rapporti B2B, molti fra i maggiori *cloud service provider* hanno di fatto imposto termini e condizioni generali in base ai quali il servizio viene fornito *as is*, senza alcuna garanzia di un determinato livello di *performance*. In tal caso, qualora il servizio divenisse indisponibile per un rilevante lasso di tempo l'utente non potrebbe dolersene né lamentare danni conseguenti (nei limiti in cui questi possano essere invocati. Sul punto v. *infra*) sempre che l'inadempimento non dipenda da dolo o colpa grave [24]. Per tale ragione è evidente che sono da preferire quei *provider* che rappresentino contrattualmente i livelli di servizio, previa una accurata valutazione da parte dell'utente della adeguatezza di tali standard di *performance* rispetto alle proprie esigenze professionali [25].
Normalmente – nei servizi commerciali che prevedono dei SLA precettivi e non meramente indicativi – l'utente è indennizzato della indisponibilità del servizio mediante crediti (talvolta addirittura limitati ad un *cap* massimo) sulla futura fatturazione ovvero attraverso una estensione della durata del servizio. Si tratta di un modo in cui il *provider* forfetizza il danno arrecato al cliente che, per parte sua, dovrà valutare previamente se il tipo di indennizzo offerto sia sensato rispetto alla propria attività ed alle prevedibili ricadute negative (in termini di danni diretti ed indiretti) della sospensione del servizio.
Nelle (a dir vero limitatissime) ipotesi in cui l'utente avesse il peso negoziale per pretendere un contratto *tailor made*, è decisamente consigliabile porre particolare attenzione alla definizione dei SLA attraverso l'attenta predisposizione di allegati tecnici da accludere al contratto come parte integrante di esso. Oltre alla definizione dei SLA in via di allegato

(questa tecnica redazionale si adatta particolarmente bene ai servizi di *cloud computing* vista la loro naturale scalabilità [26] e la possibilità quindi per le parti di emendare un contratto modificando semplicemente un allegato tecnico) è consigliabile predisporre preventivamente una accurata ricognizione tecnica e gestionale dei bisogni del cliente ed una definizione puntuale dei criteri di monitoraggio e delle procedure di verifica dei livelli di servizio e delle prestazione [27], da trasfondere in altrettanti allegati tecnici. Si verrà quindi a formare un *corpus* di documenti tecnici che, una volta acclusi al contratto e resi parte integrante dello stesso, diverranno fondamentali per inquadrare ed interpretare esattamente le prestazioni dedotte in contratto e, conseguentemente, l'ambito di responsabilità del *cloud service provider*.

La responsabilità del *provider* per mancato raggiungimento degli SLA può rappresentare un terreno molto scivoloso. Si inizi col dire che i *cloud provider* che si impegnano a mantenere un livello minimo di servizio (come spesso accade nei contratti IT, specie in quelli di *outsourcing* informatico) sovente prevedono una serie di eccezioni contrattuali che possono essere sostanzialmente ricondotte a tre tipologie: (a) forza maggiore; (b) fatto di fornitori terzi; (c) fatto degli utenti. Per l'utente è quindi essenziale esaminare con attenzione l'estensione di tali ipotesi di irresponsabilità per valutare correttamente il rischio di eventuali inadempimenti.

Nel concetto di "forza maggiore" come delineato dalla prassi contrattuale rientrano normalmente ipotesi tipiche (ed alquanto diffuse nella contrattualistica commerciale internazionale) [28] quali: *acts of God*, guerre, rivolte, sommosse o agitazioni civili, inondazioni, terremoti, incendi, scioperi o serrate, difficoltà nell'approvvigionamento di personale o di materie prime. Possono poi comparire delle clausole generali che includono nella "forza maggiore" tutti gli eventi al di fuori del controllo [29] del *provider*. L'evidente conseguenza è che la clausola di *force majeure* può assumere un grado di ampiezza anche notevole e va pertanto negoziata con grande attenzione, nonostante si tratti di una clausola c.d. *boilerplate*, vale a dire sempre presente nei modelli di condizioni generali di contratto. Ed infatti nell'ambito del *cloud computing*, potrebbero comparire fra le ipotesi di forza maggiore delle circostanze di per sé non assimilabili a tale concetto ed, in definitiva, poco accettabili per l'utente. Fra queste: guasti *hardware* (per il cliente è ragionevole pensare che il fornitore abbia debita cura delle apparecchiature informatiche con cui vengono erogati i servizi così che un semplice guasto non comprometta la continuità degli stessi [30]); interruzione di alimentazione elettrica (anche in questo caso l'utente potrebbe ragionevolmente confidare nel fatto che il fornitore sia dotato di idonei generatori di riserva); problemi di comunicazioni fra diversi punti dell'infrastruttura del fornitore (si tratta infatti di problemi risolvibili con linee di comunicazione dedicate, altamente raccomandabili nel caso di servizi così strettamente dipendenti

dalle funzionalità telematiche); guasti causati da altri utenti (è ragionevolmente confidare che il *provider* abbia tarato la "resistenza" del proprio sistema in base ad un utilizzo anche inappropriato degli altri utenti in condivisione).
Una categoria a parte di ipotesi particolarmente delicate di esclusione dalla responsabilità sono quelle connesse al *default* di sub-fornitori o fornitori terzi del *cloud provider*. In tal caso occorre comunque distinguere fra l'ipotesi di inadempimento del sub-fornitore dovuto a sua volta a cause di forza maggiore [31] (ed in tal caso l'inadempimento del *provider* mi sembrerebbe scusabile) e quella di inadempimento imputabile (a titolo di dolo o di colpa) al sub-fornitore. Qualora la responsabilità del *provider* verso il cliente fosse contrattualmente limitata anche in tale seconda categoria di eventi, è chiaro che l'utente si troverebbe ineludibilmente soggetto alle conseguenze potenzialmente pregiudizievoli di scelte tecniche o gestionali del *provider* che esulano dal suo controllo o dalla sua conoscibilità (ad esempio mancata previsione di adeguate soluzioni di *back-up* nella definizione della propria infrastruttura; scelta di sub-fornitori non affidabili; mancata previsione di rimedi contrattuali efficaci e ribaltabili, almeno in parte, sull'utilizzatore finale; clausole di limitazione di responsabilità "a monte" eccessivamente ampie;…) ed ogni rimedio contrattuale per mancato rispetto dei SLA previsto a valle sarebbe di fatto privo di significato [32].
Una ulteriore categoria di ipotesi di esclusione di responsabilità raggruppa i casi riconducibili alla responsabilità dell'utente. Appartengono a tale novero eventi come: mancato o intempestivo pagamento dei canoni del servizio; atti o omissioni dell'utente; conseguenze dell'uso di *software* (non autorizzati o non compatibili) nelle macchine *client*; violazioni dei termini d'uso da parte dell'utente. In quest'ottica sembra in linea di principio sensato escludere la responsabilità per fatto dell'utente, anche se ciò non esclude di dover prestare attenzione alla lettera del contratto (vincoli di utilizzo troppo restrittivi o limitazioni particolari all'utilizzo di *software* installati sui computer *client* potrebbero risultare anche molto pesanti per l'utente).
Infine, viene di norma esclusa la responsabilità del *provider* per mancato raggiungimento dei livelli di servizio in casi come manutenzione programmata debitamente preannunciata all'utente, atti illeciti di terzi (tipicamente attacchi *hacker* e virus), atti o richieste dell'Autorità (gli ultimi due riconducibili concettualmente alla categoria di forza maggiore).
In chiusura sul tema della responsabilità per rispetto degli SLA occorre tener presenti alcune previsioni contrattuali potenzialmente critiche e precisamente: (a) i criteri di monitoraggio dei SLA; (b) la facoltà del *provider* di modificare unilateralmente gli SLA.
Con riferimento al primo dei due punti sopra menzionati gli aspetti più delicati concernono i criteri di quantificazione dei *downtime* [33], l'obbligo

del *provider* di notificare all'utente le interruzioni del servizio [34]. Quanto al secondo punto, invece, la discrezionalità concessa al *provider* di intervenire sui SLA in corso d'opera, sebbene teoricamente giustificabile con la necessità tecnica di tenere conto – tempo per tempo – delle condizioni (anche esterne [35]) di fornitura del servizio, di fatto potrebbe esporre l'utente ad eventuali abusi [36]. Sullo specifico punto, peraltro, val la pena considerare, in prospettiva diversa, che il cliente potrebbe a sua volta pretendere la variazione dei SLA ed, in generale, degli *standard* tecnologici del servizio in corso di esecuzione del contratto e ciò al fine di ottenere un adeguamento dell'offerta al divenire della tecnica (normalmente nel settore informatico si assiste ad un incremento esponenziale delle prestazioni delle macchine e/o ad una diminuzione dei costi dell'*hardware*).
Si tratta anche in questo caso di aree contrattuali delicata che andranno attentamente verificate.

## 3. La disciplina contrattuale della *privacy* e della sicurezza informatica dei dati comunicati dall'utente al *cloud provider*.

Una seconda area di rischio per la stabilità e buona esecuzione del contratto è connessa alla capacità del *cloud provider* di garantire e mantenere la riservatezza, sicurezza, integrità e disponibilità dei dati che l'utente affida ai *data center* esterni. Si tratta di quell'ampio settore che è stato qualificato dalla dottrina come *diritto della sicurezza informatica* [37].
La sicurezza e riservatezza dei dati comunicati al *cloud provider* è, allo stato, una delle maggiori preoccupazioni dell'utente che, nel relazionarsi con il fornitore, dovrà acquisire garanzie sufficienti affinché vengano rispettati adeguati canoni di protezione. Ciò in quanto il flusso di dati riguarda informazioni che sovente consistono in dati personali [38] in quanto riferite a soggetti terzi direttamente o indirettamente individuabili. Come noto, del resto, le violazioni della disciplina sulla *privacy* possono comportare rilevantissime sanzioni amministrative e addirittura penali e, in linea di massima, l'utente del servizio *cloud* potrebbe restare esposto in prima persona a tali conseguenze sanzionatorie.
In via di premessa occorre individuare che tipo di relazione si crea fra *cloud service provider* ed utente ai fini della disciplina sulla *privacy*. Senza entrare nei dettagli di una casistica che nei fatti può diventare particolarmente complessa [39], in estrema sintesi può affermarsi che, nella stragrande maggioranza dei casi l'utente sarà titolare del trattamento (*controller* [40]) dei dati [41] da esso raccolti mentre il *cloud provider* sarà responsabile del trattamento (*processor* [42]). Il tratto distintivo, in ogni caso, dovrà essere individuato nel potere decisionale di ciascun soggetto in

merito al trattamento: in sostanza sarà titolare [43] solo colui che autonomamente *"determina le finalità e gli strumenti del trattamento di dati personali"*; così opinando, se il *provider* fosse dotato di una ampia libertà decisionale nel definire i caratteri essenziali del trattamento, non si potrebbe che riconoscere a quest'ultimo la qualità di "titolare" o di "contitolare" [44].
Alla luce di tale assetto, che converrà comunque all'utente previamente esplorare in concreto prima della selezione del *cloud service provider*, dovranno essere considerati due aspetti: nel caso di rapporto titolare-responsabile, infatti, l'utente dovrà [45] principalmente: (a) assicurarsi di avere un controllo effettivo sui dati; (b) selezionare un responsabile del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare; (c) assicurarsi del rispetto di tali misure. Se il rapporto fra utente e *cloud provider* si delinea invece come fra due titolari autonomi o fra contitolari, il problema più rilevante è quello del trasferimento all'estero dei dati personali [46].
Nell'ipotesi più frequente, quindi, l'utente dovrà principalmente accertarsi di essere nelle condizioni di esercitare un effettivo controllo sui dati comunicati al *cloud provider* ai fini del rispetto delle misure di sicurezza imposte al *provider*. È intuibile come si tratti di un'impresa alquanto ardua, soprattutto in considerazione del normale sbilanciamento fra i poteri negoziali delle parti, delle asimmetrie informative esistenti e, non ultimo, della impossibilità (talvolta) per lo stesso *provider* di indicare con sicurezza dove i dati esattamente risiedano [47]. È tuttavia consigliabile all'utente svolgere una verifica preventiva (che nelle ipotesi più articolate potrebbe giungere sino alle soglie di una vera e propria *due diligence* [48] sull'infrastruttura, sul personale e sulle procedure del *provider*) al fine di prendere atto che gli standard di sicurezza del *provider* siano ragionevoli o comunque commisurati alla rilevanza dei dati affidatigli [49]. Naturalmente le forme di questa verifica potranno essere le più varie: dal semplice studio ed approfondimento (e comparazione) delle offerte tecniche dei vari *provider* ad una interazione vera e propria (ove concretamente possibile) con questi ultimi (esplicite richieste di informazioni, questionari, incontri fra i rispettivi tecnici, ecc. [50]), tutto al fine di chiarire i profili di gestione dei dati nel sistema del *cloud provider* e garantire (nei limiti del possibile) all'utente un adeguato grado di controllo sul flusso dei dati. Un importantissimo elemento da considerare nella verifica preliminare del fornitore del servizio *cloud* è poi il rispetto, da parte di quest'ultimo, di idonei *standard* specificamente relativi alla gestione della sicurezza delle informazioni, in particolare i c.d. ISO/IEC 27001 (certificabile da organismi terzi e quindi effettivamente verificabile dall'utente) e ISO/IEC 27002 (complementare al primo soprattutto nell'ottica dell'implementazione dei controlli, ma non certificabile da organismi terzi) [51]. Da notare che il

rispetto degli *standard* di sicurezza sopra indicati o il possesso delle relative certificazioni, ove non espressamente rappresentato e garantito in contratto, non può essere considerato in sé un parametro di adempimento o non adempimento delle obbligazioni del *cloud provider* in ordine alla sicurezza e riservatezza dei dati: in tal caso, infatti, il cliente potrà assumere come riferimento il livello di diligenza professionale degli operatori del settore e le *best practices* da questi seguite, così che solo lo scostamento del *provider* dallo *standard* ragionevolmente atteso potrà assumere rilevanza giuridica.
Altro aspetto fondamentale per l'esatta delimitazione della responsabilità fra le parti di un contratto *cloud* è il modo in cui queste ultime affrontano il nodo del flusso transfrontaliero dei dati. È infatti noto che la disciplina comunitaria è particolarmente restrittiva rispetto a tale fenomeno [52] che nel settore in commento rappresenta praticamente la regola. Il trasferimento dei dati verso un Paese extra UE è infatti possibile solo *"se il paese terzo di cui trattasi garantisce un livello di protezione adeguato"* [53]. Ad oggi sono molto pochi i Paesi inclusi in tale novero: Svizzera, Ungheria, Canada, Argentina, Baliato di Jersey, Isola di Man, Isole Far Øer, Principato di Andorra, e Stato di Israele [54]. I trasferimenti di dati verso gli Stati Uniti, invece, si ritengono in linea con la disciplina comunitaria se avvengono in direzione di imprese che aderiscono ai cosiddetti *Safe Harbor Privacy Principles* [55]. Altra modalità recentemente [56] prevista dal Codice Privacy per il (legittimo) trasferimento dei dati all'estero è costituita dal ricorso alle cosiddette *Binding Corporate Rules* o BCR (*"regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo"* [57]) che disciplinino la comunicazione di dati fra soggetti giuridici diversi, di Paesi diversi e che, se approvate dall'Autorità garante del Paese esportatore o da più Autorità, dovrebbero consentire il trasferimento verso Paesi terzi, con un adeguato livello di sicurezza [58].
Nel caso di Paesi che esulino dall'elenco sopra richiamato ovvero di trasferimento di dati a imprese statunitensi che non aderiscono al *Safe Harbor* la soluzione preferibile (per l'utente del servizio *cloud*) è la fissazione per contratto di garanzie minime a difesa dei soggetti interessati dal trattamento e la previsione di clausole di manleva per pregiudizi (risarcimenti e sanzioni amministrative) in cui l'utente *cloud* dovesse incorrere per mancato rispetto del fornitore di tali misure. In tal senso soccorrono utilmente le clausole tipo approvate dalla Commissione Europea [59] che hanno la duplice finalità di garantire una adeguata tutela dell'interessato, da un lato, e di responsabilizzare l'esportatore dei dati. Ai fini della mappatura della responsabilità delle parti di un contratto *cloud* munito delle suddette clausole, è opportuno citare la clausola 3 ("Clausola del terzo beneficiario") e la clausola 6 ("Responsabilità"): in base al combinato disposto di tali pattuizioni, infatti, l'interessato (persona fisica o giuridica cui si riferisce il dato oggetto di trattamento e di esportazione)

potrà far valere i propri diritti (anche in via risarcitoria e, se del caso, per tramite di associazioni o organizzazioni rappresentative [60]) nei confronti dell'esportatore, dell'importatore (*"qualora l'esportatore sia scomparso di fatto o abbia giuridicamente cessato di esistere"*) e, addirittura, del subincaricato (*subprocessor*) del trattamento (*"qualora sia l'esportatore che l'importatore siano scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi"*). L'importatore, inoltre, non potrà far valere la violazione degli obblighi contrattuali ad opera del subincaricato [61] al fine di escludere la propria responsabilità. In base alle clausole tipo in commento (clausola 9), inoltre, la legge applicabile al contratto sarà quella del luogo di stabilimento dell'esportatore (quindi nei contratti *cloud* tipicamente la disciplina di un Paese europeo).
La disciplina europea sulla *privacy* ha tuttavia spinto molti dei maggiori operatori *cloud* a dotarsi di *data center* siti in Paesi europei e ciò al fine di agevolare la propria penetrazione commerciale nel mercato europeo. Se questo risolve alcuni dei problemi sopra evidenziati, ne fa sorgere di nuovi (e più complessi) nel caso in cui il *cloud provider* stabilito nell'Unione Europea si avvalga di soggetti terzi extra UE in qualità di subincaricati del trattamento dei dati. Mancano in questo caso delle clausole tipo approvate dalla Commissione. [62] Sono state quindi ventilate alcune soluzioni [63] fra le quali: un rapporto contrattuale diretto fra il titolare [64] (europeo) ed il subincaricato (non europeo) che preveda l'inclusione delle clausole tipo di cui alla decisione 2010/87/CE (in questo caso il subincaricato viene trattato alla stregua dell'incaricato importatore); un chiaro mandato all'incaricato (europeo) di usare le clausole di cui alla decisione 2010/87/CE nel suo rapporto contrattuale con il subincaricato (non europeo) [65]; contratti *ad hoc*, previa approvazione delle competenti autorità del Paese dell'esportatore.
Il problema concreto dell'uso delle clausole standard è che, se da un lato esse consentono al *cloud provider* di tranquillizzare il cliente rendendolo in linea con i propri vincoli legislativi, dall'altro esporrebbero i *provider* ad uno *standard* di responsabilità ben più elevato di quello che gli stessi sarebbero disponibili ad accettare in una "normale" negoziazione contrattuale (e ciò soprattutto alla luce della clausola "del terzo interessato" su cui vedi *supra*). Il dubbio è se la responsabilità del *provider* verso l'utente per mancato rispetto da parte del primo delle prescrizioni sulla sicurezza dei dati possa essere limitata [66] (ovviamente senza pregiudizio dei diritti del "terzo interessato") oppure se siffatta limitazione, non essendo prevista nel *set* di clausole tipo, possa essere ritenuta da un'Autorità garante come una inaccettabile violazione rispetto allo schema precostituito e perciò stesso far venir meno il salvacondotto per il cliente. A mio avviso tale eventualità non dovrebbe verificarsi in quanto – anche in base ai considerando della decisione 2010/87/CE – la funzione delle clausole come già detto) è quella di assicurare la tutela dei terzi interessati

e di sensibilizzare l'esportatore alla propria responsabilità (in chiave risarcitoria e sanzionatoria); se quindi non viene pregiudicato il diritto dell'interessato ad agire nei confronti dell'importatore (nei limiti previsti dalla clausola 3, sopra ripercorsa), eventuali pattuizioni volte ad escludere la responsabilità dell'importatore (il *cloud provider*) verso l'esportatore (il cliente *cloud*) non farebbero che rafforzare la responsabilità dell'esportatore e perciò non sembrano intrinsecamente disallineate rispetto agli obiettivi della decisione.

## 4. I dati come beni aziendali: problemi di sicurezza ed integrità delle informazioni sul *cloud*.

Una terza area critica è quella della integrità e sicurezza dei dati dell'utente *cloud*, viste non nell'ottica del rispetto delle norme di ordine pubblico a tutela della *privacy* quanto piuttosto del diritto patrimoniale dell'utente stesso ad mantenere il controllo, la disponibilità e la segretezza di tali informazioni.
Ed infatti l'utente *cloud* (in particolar modo se parliamo di utente *business*), perdendo di fatto il controllo dei propri dati, ha un rilevante ed insopprimibile interesse a preservare il proprio patrimonio informativo in quanto bene *lato sensu* aziendale [67]. Tale patrimonio, infatti, resta esposto ad una serie di rischi [68] (tipicamente connessi all'uso degli strumenti informatici e telematici ed alcuni dei quali sono stati già ripercorsi nella presente relazione) che mettono a repentaglio la disponibilità o il valore dei propri *asset* informativi; fra questi: comportamenti dolosi o negligenti del *provider* o di suoi dipendenti, difetti o malfunzionamenti del sistema informatico del *provider*, eventi naturali distruttivi, comportamenti dolosi di terzi [69] (*hacker* e *virus*).
Del resto è noto che le informazioni aziendali riservate dotate di determinati requisiti costituiscono un vero e proprio bene immateriale su cui il titolare può vantare ed esercitare dei diritti dominicali. In Italia, infatti, sono tutelate come bene giuridico [70] le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali che abbiano le seguenti caratteristiche: (a) siano segrete (in quanto non siano note o facilmente accessibili agli operatori del settore) [71]; (b) abbiano un valore economico in quanto segrete [72]; (c) siano sottoposte a misure di segretezza adeguate da parte delle persone al cui legittimo controllo sono soggette [73].
Dal punto di vista comparatistico, la disciplina interna in tema di segreto aziendale appare simile a quella statunitense sancita dall'*Uniform Trade Secrets Act* del 1979 che, ai fini dell'esercizio del diritto, richiede al soggetto leso di dimostrare che le informazioni siano state acquisite da terzi illegalmente (*misappropriation*) e cioè mediante *improper means* o

*breach of confidence* [74]. Nel Regno Unito, pur in assenza di un provvedimento legislativo specifico sui segreti aziendali che qualifichi gli stessi come un bene di proprietà intellettuale, la giurisprudenza sembra orientata decisamente nel senso di dare tutela al titolare delle informazioni in tutti i casi in cui vi sia stata una indebita o illegittima appropriazione ed utilizzazione delle stesse.
È quindi evidente che il tema è assai rilevante in quanto eventuali brecce nella sicurezza del *cloud provider* potrebbero causare l'azzeramento del valore economico di un *asset* aziendale e, contemporaneamente, a un danno competitivo [75] all'utente del servizio.
Ma la violazione della sicurezza dei dati relativi all'utente potrebbe rilevare anche quando essa abbia ad oggetto dati privi dei requisiti per poter essere qualificate come informazioni aziendali riservate, oggetto di un diritto assoluto di natura dominicale. È il caso della c.d. *privacy* delle persone giuridiche: l'impresa potrebbe infatti reclamare un danno per violazione di un diritto soggettivo assoluto (il diritto alla *privacy*) come conseguenza della indebita diffusione di informazioni ad essa riferibili, suscettibili – ad esempio – di arrecare discredito alla propria attività o al proprio buon nome commerciale. Si è già osservato che sono molto pochi gli ordinamenti che estendono la disciplina prevista per le persone fisiche anche alle persone giuridiche, enti ed associazioni [76]. Tuttavia, è stato osservato che anche in quei Paesi in cui tale specifica protezione non sia espressamente prevista si potrebbe ricostruire un diritto alla "*privacy* collettiva" come un diritto dei membri di tale collettività *"a non essere turbati nella vita quotidiana attraverso l'indebita diffusione di notizie riferite alla collettività"* [77]. La specifica questione è in vero complessa e sicuramente di per sé esorbita l'oggetto di questa relazione, ma tuttavia utilissima per aprire un ulteriore angolo di visuale sui rischi connessi all'utilizzo di servizi *cloud* e sulle conseguenti eventuali responsabilità del *provider*.
Quanto sopra detto sui problemi potenzialmente connessi alla gestione dei dati e delle informazioni fa comprendere come il tema della ripartizione dei relativi rischi e responsabilità sia cruciale nella scelta del *cloud service provider* o nella negoziazione delle relative condizioni contrattuali (quando ciò è possibile).
Le condizioni contrattuali *standard* offerte dai *cloud provider* sono infatti di norma attentamente tarate al fine di evitare (o almeno ridurre al massimo) qualsiasi responsabilità connessa alla gestione dei dati (si rinvengono spesso nelle condizioni generali di contratto clausole che sanciscono che la responsabilità per il mantenimento della riservatezza e dell'integrità dei dati è del cliente; nella migliore delle ipotesi tale *disclaimer* si accompagna ad una generica dichiarazione del *provider* che comunque assicura i propri *best efforts* per preservare i dati) [78].

Si tratta evidentemente di condizioni difficilmente accettabili per un utente *business*, che potrebbe facilmente trovarsi a dover fronteggiare danni (sotto forma di danno emergente e di lucro cessante) davvero molto cospicui. La casistica di oneri, costi e danni connessi ad una violazione dei dati può infatti essere davvero molto ampia. Fra questi val la pena citare:
a) i costi della notifica della violazione agli interessati (clienti, fornitori, *partner* commerciali, dipendenti,…) che – ancorché non sempre obbligatoria a termini di legge – può essere nei fatti utile o essenziale ai fini di ridurre le conseguenze dannose dell'evento (per esempio per preservare il buon nome commerciale dell'azienda ovvero per consentire ai diretti interessati di porre rimedio, per quanto possibile, all'incidente occorso, limitando quindi l'impatto dei danni potenziali);
b) i costi di assistenza agli interessati (ancora più elevati nel caso di notifica sistematica della violazione);
c) risarcimenti per gli interessati (ad es. clienti dell'utente *cloud*) nel caso in cui questi dimostrino di aver subito un danno;
d) danno d'immagine (anche sotto forma di perdita di avviamento. Si tratta di un danno difficile da provare in via giudiziale, ma che può emergere con evidenza nel caso in cui, a seguito di una violazione molto grave della sicurezza, l'azienda registri un drastico calo di fatturato o un crollo delle proprie quotazioni);
e) costi di ricostituzione della base dei dati (nel caso di "semplice" danneggiamento).
Con riferimento a tali tipologie di danni, se è comprensibile la resistenza del *provider* ad accollarsi danni indiretti come calo di fatturato, perdita di avviamento, danno d'immagine (sul punto specifico si veda *infra*), è tuttavia più agevole per l'utente *cloud* pretendere una copertura per i costi diretti (notifica, assistenza, ricostituzione dei dati) che è costretto a sostenere a seguito della violazione dei dati. Inoltre si potrà ricorrere convenzionalmente ad idonee clausole di manleva che permettano all'utente di ribaltare sul *provider* eventuali richieste risarcitorie di terze parti.
È tuttavia evidente che, per la stessa natura dei servizi *cloud*, una violazione della sicurezza dei dati interesserà presumibilmente tutti gli utenti del servizio, con estensione "a macchia d'olio" delle eventuali responsabilità risarcitorie e conseguenze potenzialmente esiziali per il *cloud provider*. Per tale ragione non sembra francamente possibile che quest'ultimo accetti una responsabilità illimitata che tenderà, nella migliore delle ipotesi, a ridurre con idonei *cap* (la cui ragionevolezza, per altro verso, dovrà essere attentamente valutata dal cliente).

## 5. Soluzioni assicurative contro i rischi del *cloud computing*.

Sempre in tema di responsabilità del *cloud service provider*, una breve notazione merita la risposta del mercato assicurativo alla crescente domanda di servizi sulla nuvola. Molte compagnie assicurative, infatti, hanno sviluppato prodotti specifici, eliminando per altro verso la copertura per danni connessi alla perdita di dati e per violazioni alla riservatezza nei sistemi elettronici dalle normali polizze di responsabilità civile (CGL – *commercial general liabilty*) e dalle polizze c.d. "errori ed omissioni" (E&O). Sono nate quindi delle polizze generalmente denominate "errori e omissioni tecnologici" (Tech E&O) che possono essere sottoscritte sia dall'utente del servizio *cloud* sia dal *provider*. È bene tuttavia evidenziare che, allo stato dell'arte, la maggior parte di tali polizze esclude la copertura per danni della cui responsabilità l'assicurato si sia fatto volontariamente carico in via contrattuale, così che – qualora il contratto con il cliente ne prevedesse – sarà necessario negoziare con la compagnia delle espresse eccezioni. Esistono poi delle soluzioni ibride di polizze *Tech E&O* e *Cyber Liability* che assicurano sia l'esposizione verso terzi sia quella verso la propria controparte contrattuale, coprendo una serie di costi come le spese di notifica della violazione, i servizi di monitoraggio e l'interruzione del servizio nonché servizi aggiuntivi come tutela legale specialistica, copertura di spese di perizie tecniche e di indagini, supporto nelle pubbliche relazioni, supporto IT.

## 6. Violazione del contratto e risarcimento del danno.

Senza alcun dubbio l'implicazione più rilevante nel caso di inadempimento contrattuale di servizi *cloud* è fino a che punto debba estendersi l'obbligo risarcitorio. Per tale ragione gli schemi contrattuali normalmente adottati nel settore pongono particolare attenzione al tema dell'esonero e/o della limitazione della responsabilità, anche perché (come già osservato) in ambiente *cloud* un problema nell'erogazione del servizio o nella sicurezza ed integrità dei dati finisce inevitabilmente per ripercuotersi su un gran numero di utenti (se non addirittura su tutti).
In linea di massima il debitore inadempiente è sempre responsabile dei danni diretti e prevedibili. Il problema dei danni indiretti ed imprevedibili, invece, oltre ad essere di gran lunga più delicato (per via del potenziale indiscriminato ampliamento della responsabilità), è affrontato in maniera diversa dai vari sistemi giuridici. È questa la ragione per cui, prima di redigere una clausola di esonero o di limitazione dalla responsabilità, è opportuno conoscere con esattezza la disciplina applicabile.
In Italia, come noto, in caso di inadempimento (o di ritardo nell'adempimento) il debitore è tenuto a risarcire il creditore di tutti i danni

prevedibili al momento in cui è sorta l'obbligazione, a meno che l'inadempimento non derivi da dolo del debitore (art. 1225 cod. civ.). Analoga impostazione restrittiva mostrano la legge francese e belga. Anche la *common law* sembra improntata al criterio (per la verità di derivazione romanistica) della prevedibilità del danno, come enunciato nei principi della notissima sentenza *Hadley-Baxendale* [79]. Nel diritto tedesco e scandinavo, invece, vige la dottrina della "causalità adeguata" secondo cui deve essere risarcito qualunque danno che derivi in modo adeguato da un inadempimento contrattuale.

In base all'art. 74 della Convenzione di Vienna sulla compravendita internazionale di merci [80] *"il risarcimento del danno per l'inadempimento del contratto da parte di un contraente consiste in una somma uguale alla perdita, incluso il mancato guadagno, subita dall'altro contraente in conseguenza dell'inadempimento. Il risarcimento del danno non può essere superiore alla perdita che la parte inadempiente aveva previsto o avrebbe dovuto prevedere al momento della conclusione del contratto avuto riguardo ai fatti e alle circostanze che egli allora conosceva o avrebbe dovuto conoscere come possibile conseguenza dell'inadempimento".*

Secondo i principi Unidroit *"il creditore ha diritto al risarcimento integrale del danno subito in conseguenza dell'inadempimento. Il danno comprende sia ogni perdita sofferta che ogni mancato guadagno, tenuto conto dei vantaggi economici che il creditore ha ottenuto evitando spese e danni"* [81] con la precisazione che *"la parte inadempiente è responsabile solo per il danno che ha previsto o poteva ragionevolmente prevedere al momento della conclusione del contratto come possibile conseguenza dell'inadempimento"* [82].

In linea di massima si tenga presente che di norma le clausole che escludono o limitano la responsabilità per danni indiretti e/o imprevedibili non sembrano in sé e per sé minacciate da motivi di invalidità distinti da quelli che pesano sulle clausole di esonero o limitative in generale (dolo, colpa grave, irragionevolezza,…).

Rispetto ad un contesto che – fatte salve alcune divergenze, anche dovute alla concreta applicazione dei principi da parte delle corti – appare improntato al criterio della prevedibilità del danno, corre l'obbligo segnalare il par. 2-719 dello *Uniform Commercial Code* statunitense secondo cui *"consequential damages may be limited or excluded unless the limitation or exclusion is unconscionable"*.

Inoltre si rammenti che in molte giurisdizioni (in Italia ed, in generale, nei Paesi europei) le clausole limitative della responsabilità sono soggette ad una stringente disciplina legislativa nei casi in cui siano contenute in condizioni generali di contratto unilateralmente predisposte e non negoziate (come normalmente accade per i servizi di *cloud computing*), anche se il limite della validità delle stesse viene sovente rinvenuto dalle corti di merito nella ragionevolezza delle stesse.

---

Note:

[*] Il presente saggio è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.

[**] Relazione presentata al convegno "Cloud Computing e Diritto – Questioni attuali e sfide future", organizzato dall'Università Commerciale L. Bocconi, 17 maggio 2012.

[1] Marchini, *Cloud Computing: a Practical Introduction to the Legal Issues*, London, 2010, pag. 13.

[2] Regolamento (CE) n. 593/2008 del Parlamento Europeo e del Consiglio del 17 giugno 2008 sulla legge applicabile alle obbligazioni contrattuali («Roma I»), pubblicato in G.U.C.E. n. L 177/6 del 04/07/2008.

[3] Regolamento (CE) n. 864/2007 del Parlamento Europeo e del Consiglio dell'11 luglio 2007 sulla legge applicabile alle obbligazioni extracontrattuali («Roma II»), pubblicato in G.U.C.E. n. L 199/40 del 31/07/2007. Quest'ultima ipotesi ricorre evidentemente nel caso in cui la lite insorga fra soggetti fra di loro non vincolati contrattualmente, come ad esempio accadrebbe nel caso in cui una persona fisica o giuridica lamentasse un danno connesso al contegno doloso o colposo del *cloud provider* (l'ipotesi tipica è la violazione della *privacy*) o anche del cliente del servizio *cloud* (anche se in questa seconda ipotesi è facile che sussista un rapporto contrattuale fra il cliente *cloud* e il soggetto cui il dato si riferisce).

[4] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) pubblicata in Gazzetta Ufficiale n. L 201 del 31/07/2002.

[5] V. *supra*.

[6] 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»), pubblicata in Gazzetta ufficiale n. L 178 del 17/07/2000 pag. 0001 - 0016

[7] Per un confronto fra i differenti approcci, calato nel contesto digitale, si veda Mantelero, *Privacy digitale*, in *Manuale di informatica giuridica e diritto delle nuove tecnologie*, a cura di Durante e Pagallo, Torino, 2012m, pp. 159 e ss.. Con specifico riferimento al *cloud computing* Chris Hoofnagle, *Senior Fellow* presso il *Berkeley Center for Law & Technology*, ha sottolineato che negli Stati Uniti il Quarto Emendamento alla Costituzione protegge senza dubbio i dati sui PC o i *devices* mobili in possesso dell'utente, ma quando, come nel *cloud computing*, i dati personali sono trasferiti a terzi la loro tutela diventa sensibilmente più

affievolita (Hoofnagle, *Consumer Protection in Cloud Compunting Services*, Atti del convegno organizzato da *Consumer Federation of America* il 20-22 giugno 2010 alla New York University School of Law, successivamente pubblicato in *Consumatori, Diritti e Mercato*, 1/2011, pag. 92. Articolo disponibile anche su http://www.altroconsumo.it/nt/nc/news/cloud-computing-consumatori-diritti-e-mercato-16-n538300/download?ressourceUri=BFC2FB4EE5A5E2D9EC8106D7F3C122B8E669A2B6).

[8] In questo senso il monito delle istituzioni comunitarie e, in Italia limitatamente al problema della privacy, i rilievi del Garante per la protezione dei dati personali (v. scheda di documentazione "Cloud computing: indicazioni per l'utilizzo consapevole dei servizi" presentata in occasione della Relazione sul quattordicesimo anno di attività e sullo stato di attuazione della normativa sulla privacy). Giova ricordare che Neelie Kroes, Vice Presidente della Commissione Europea e Commissario per l'Agenda Digitale ha a più riprese osservato come il cloud computing non sia un fenomeno da imbrigliare con regole scritte nella pietra e ciò sia per ragioni di intriseci limiti della tecnica legislativa (incapace di seguire tempestivamente l'evoluzione rapidissima di certa tecnologia) sia per la vitale importanza dell'economia digitale che va frenata solo dopo aver accuratamente valutato il *trade-off* in termini di oneri e praticabilità.

[9] Decreto legislativo 6 settembre 2005, n° 206 e s.m.i., pubblicato in G.U. 08.10.2005. L'art. 143 del Codice prevede che *"i diritti attribuiti al consumatore dal codice sono irrinunciabili. È nulla ogni pattuizione in contrasto con le disposizioni del codice"*.

[10] v. Relazione di accompagnamento al decreto legislativo 6 settembre 2005, n. 206.

[11] *Ex multis* Tribunale Roma, 30/11/2009, in *Foro it.* 2011, 1, 256; Tribunale Trieste, 20/09/2006, in *Corriere del merito* 2007, 2, 178 (nota BATTELLI); Tribunale Catania, 05/01/2004, in *Foro it.* 2004, I, 262; Tribunale Roma, 05/11/2003, in *Riv. dir. comm.* 2004, II, 1 (nota FABBIO). Inserire giurisprudenza conferente.

[12] La legge parla di *"eccessivo squilibrio di diritti ed obblighi"*, locuzione che riecheggia il *"significativo squilibrio di diritti ed obblighi"* in tema di clausole abusive. La dottrina ha tuttavia chiarito che le due formulazioni non sono conciliabili ai fini di una interpretazione sistematica: in questo senso v. Pinto, *L'abuso di dipendenza economica «fuori dal contratto» tra diritto civile e diritto antitrust*, in *Riv. dir. civ.*, 2000 pag. 394; Colangelo, *L'abuso di dipendenza economica tra disciplina della concorrenza e diritto dei contratti – Un'analisi economica e comparata*, Torino, 2004, pag. 79; Benucci, *Le prime pronunce in tema di «*abuso di dipendenza economica*»*, in Vettori (a cura di), *Concorrenza e Mercato*, pag. 485; *contra* Prosperi, *Il contratto di subfornitura e l'abuso di dipendenza economica. Profili ricostruttivi e sistematici*, Napoli, 2002, pag. 297.

[13] Oppo, *Princìpi*, Torino, 2001, pag. 43; sul punto anche Mazziotti di Celso, *Abuso di dipendenza economica*, in G. Alpa - A. Clarizia (a cura di), *La Subfornitura*, Commento alla legge 18 giugno 1998, n. 192, Milano, 1999, pag. 247. Secondo Pinto, *op. cit.*, pag. 405 quello della reale sostituibilità sarebbe l'unico criterio legale di accertamento dell'abuso di dipendenza economica (fermo restando che nel concreto atteggiarsi dei rapporti se ne potrebbero riscontrare altri).
[14] Nella relazione di accompagnamento alla legge 192/1998 si evidenziava chiaramente che l'art. 9 trova quale *«referente comparatistico [...] il paragrafo 26, comma 2, secondo periodo [ora § 20, comma 2], della normativa antimonopolistica tedesca (GWB), ripresa dal legislatore francese nell'art.8, lettera b), dell'ordinanza 1° dicembre 1986, n.1243 [ora art. L. 420 – 2 del Code de commerce]»*.
[15] Si rammenta in proposito che nel caso *Kingsway Hall Hotel v. Red Sky IT (Houslow)* [2010] EWHC 965 (TCC). In tale precedente è emerso il principio di diritto secondo cui in un contratto per servizi IT concluso fra un imprenditore non specialista del settore ed un imprenditore specialista determinate clausole, sebbene racchiuse in condizioni generali di contratto, possono considerarsi inique e sleali (*unfair*) e non efficaci (*unenforceable*). Sebbene il caso concreto non riguardasse servizi *cloud* il ragionamento della corte, appuntandosi sulla elevata specificità di determinate condizioni contrattuali e sulla asimmetria conoscitiva delle parti, è assolutamente applicabile alla verifica dei contratti di *cloud computing*. Il precedente è riportato in Bradshaw, Millar e Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 63/2010, pag. 16 e ss. Disponibile su http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374 e successivamente pubblicato, con alcuni aggiornamenti, in *International Journal of Law and Information Technology*, 2011, 19 (3), pagg. 187-223.
[16] Tali principi – come noto – dettano specifiche regole (ancorché di *soft law*) in tema di conclusione del contratto, vizi del volere, invalidità, interpretazione, contenuto del contratto, adempimento, sopravvenienze, inadempimento, e risoluzione, e la cui essenza è stata proprio rinvenuta nell'opera di coordinamento delle pratiche internazionali con i principi generali del diritto universalmente accolti, così da contemperare le caratteristiche proprie della *lex mercatoria* quale diritto unilateralmente creato dalla classe imprenditoriale con le esigenze di protezione del contraente debole
[17] Tale disposizione consente, infatti, di chiedere l'annullamento o la modifica del contratto o di una singola clausola che attribuisca ad una parte un vantaggio eccessivo qualora detto vantaggio appaia ingiustificato in base ad una serie di fattori di natura soggettiva (imperizia, ignoranza,

inesperienza o mancanza di abilità a trattare) ed oggettiva (natura e scopo del contratto). I presupposti per agire in base a tale disposizione sono, pertanto, rappresentati da un lato dal vantaggio eccessivo a favore di una parte, che secondo il commento ufficiale, si ha quando vi sia una ragguardevole disparità di valore tra le prestazioni tanto che un tale squilibrio sia "*so great as to shock the coscience of a reasonable person*", e dall'altro dalla mancanza di giustificazione di tale vantaggio.
[18] È comunque quest'ultima una valutazione da compiersi in concreto e che, allo stato del mercato (in pieno fermento), non può darsi per acquisita definitivamente.
[19] In ultima analisi rilevano le modifiche delle condizioni – direttamente o indirettamente – economiche (prezzi, interessi, termini di pagamento,…).
[20] In questa sede si intende per *lock in* "assoluto" il caso di impossibilità tecnica assoluta per l'utente di esportare i dati immagazzinati presso il *cloud provider* in un formato idoneo a permetterne il caricamento in propri *server* o presso altri *cloud provider*. Per lock in "relativo", invece, si vuol indicare il caso in cui il cambio di fornitore (necessitato dall'ipotetica impennata dei prezzi o dal deterioramento delle condizioni economiche per l'utente) implichi dei costi rilevanti per il cliente. Il tema del *lock in*, sebbene in chiave *antitrust*, verrà approfondito in una successiva relazione e quindi non è il caso in questa sede di dilungarsi.
[21] Esiste allo stato una interessante attività di studio svolta da organizzazioni e consorzi industriali ed accademici finalizzata ad una sorta di "negoziazione intermedia" fra fornitori e utenti; un esempio è la SLA@SOI (http://sla-at-soi.eu/), un consorzio di ricerca finanziato dall'Unione Europea nell'ambito del VII Programma Quadro. Fra i più recenti risultati di questi studi, v. Wieder, Butler, Theilmann and Yahyapour, *Service Level Agreements for Cloud Computing*, Springer, 2011.
[22] Zincone, *Il contratto di outsourcing: natura, caratteristiche, effetti*, in *Dir. aut.*, 2002, pag. 391.
[23] Belisario, *Diritto sulle nuvole – profili giuridici del cloud computing*, in *Informatica giuridica – collana diretta da Michele Iaselli*, eBook di Altalex, pag. 18. Il dato emerge con evidenza anche in Bradshaw, Millar e Walden, *op. cit.*, pagg. 38-39.
[24] Il principio è sancito nel diritto italiano dall'art. 1229, I co., cod.civ., ma è un fatto che la maggior parte degli ordinamenti giuridici privino di efficacia le clausole di esonero o limitative della responsabilità qualora queste risultino da ipotesi di dolo e, spesso, anche di colpa grave del debitore. In tal senso – e per un approfondita analisi di diritto comparato, si veda Fontaine-De Ly, *La redazione dei contratti internazionali a partire dall'analisi delle clausole*, Milano, 2008, pag. 471 e pagg. 492 e ss. in cui si rileva che la clausola di esonero dalla responsabilità per dolo o colpa grave è radicalmente inefficace, ad esempio, secondo il diritto francese e tedesco e che la *common law*, invece, fa leva sulla (complessa) dottrina della

*fundamental breach*, sanzionando con l'inefficacia quella limitazione che finirebbe per svuotare il contratto del suo contenuto, incidendo su una prestazione di fondamentale importanza, previa una valutazione del carattere "ragionevole" di tale clausola (*Uniform Commercial Code* statunitense e *Unfair Contract Terms Act* inglese).

[25] Nella prassi accade sovente che, anche nei casi in cui le condizioni contrattuali contemplino dei SLA, questi ultimi siano espressi con due valori: uno più elevato, che rappresenta un obiettivo (del cui eventuale raggiungimento il fornitore può fregiarsi in sede commerciale) ed un altro, più basso, il cui mancato raggiungimento rappresenta un inadempimento rilevante. Il cliente dovrà quindi prestare particolare attenzione a quest'ultimo valore che rappresenta il vero parametro su cui potrà contare come creditore della prestazione. Naturalmente va valutata l'incidenza delle eventuali clausole di esonero dalla responsabilità apposte dal *provider* nelle condizioni generali di contratto. Anche sul punto si veda la puntuale analisi presente in Bradshaw, Millar e Walden, *op. cit.*, pagg. 38-39: alcuni *provider* contemplano fra le cause di esclusione dalla responsabilità per mancato rispetto degli SLA atti o fatti come: mancato o intempestivo pagamento dei canoni; atti o omissioni dell'utente; conseguenze dell'uso di *software* nelle macchine *client*; manutenzione programmata debitamente preannunciata all'utente; forza maggiore; inadempimenti, atti o omissioni di eventuali terzi *provider* a monte; atti di terzi (tipicamente attacchi *hacker* e virus); violazioni dei termini d'uso da parte dell'utente; atti o richieste dell'Autorità. La giurisprudenza anglosassone sembra tuttavia orientata a riconoscere maggior tutela all'utente (anche professionale) che si trovi a "subire" delle clausole di esonero dalla responsabilità del fornitore, quando sussista una *special relationship* fra le parti (intendendosi per tale quella relazione che si instaura fra due soggetti uno dei quali sia in situazione di dipendenza tecnologica dall'altra) ovvero un *unequal bargaining power* (v. *Empire One Telecommunications Inc. v. Verizon New York Inc.* – N.Y.S. 3d, Nov. 2, 2009 NYLJ, p. 21, col. 3-4).

[26] Per "scalabilità" si intende la caratteristica di un dispositivo *hardware* o *software* che consente la sua estensione con ulteriori capacità e funzionalità nel caso di necessità future. Un sistema si dice scalabile quando è possibile aggiungere ulteriori funzionalità senza doverne modificare le caratteristiche fondamentali.

[27] È stato correttamente osservato che tali procedure, oltre che essenziali per un controllo costante della corretta esecuzione del contratto, sono utilissime per prevenire l'insorgere di controversie (Tosi, *Il contratto di outsourcing di sistema informatico*, Milano, 2001, pagg. 25 e ss.).

[28] Si tratta, come detto, di ipotesi *standard*, la cui effettiva previsione non sembra suscitare particolari criticità.

[29] Occorre prestare attenzione alla differenza fra le locuzioni *"beyond the control"* e *"beyond the reasonable control"* (o simili) in quanto nella prassi anglosassone il canone della ragionevolezza è suscettibile di spostare considerevolmente i termini della responsabilità del *provider*.
[30] Un singolo guasto *hardware* potrebbe non avere conseguenze pratiche concrete sulla continuità del servizio se il sistema del fornitore fosse adeguatamente ridondato.
[31] In senso stretto.
[32] Si pensi al caso di un servizio SaaS costruito sull'offerta di un *provider* PaaS. Se l'inadempimento del SaaS fosse scusato in caso di inadempimento (*tout court*) del PaaS è evidente che lo standard di servizio diventerebbe di fatto quello del PaaS a prescindere dalle rappresentazioni e garanzie del SaaS *provider*. L'esempio è in Marchini, *op. cit.*, pag. 121.
[33] Può accadere che ai fini del rispetto degli SLA vengano espressamente ritenute rilevanti interruzioni superiori ad una certa durata minima, sulla base del presupposto implicito che al di sotto di tale durata l'evento non causerebbe un danno sensibile all'utente. È evidente che previsioni del genere rendono ancor più indicativi gli SLA rappresentanti in contratto.
[34] Anche in questo caso possono rinvenirsi clausole che richiedano all'utente di segnalare al *provider* la caduta del servizio e di dare evidenza documentata della impossibilità di utilizzarlo. La funzione delle clausole siffatte sembra quella di "scremare" gli eventuali *outages* rilevanti da quelli che non sono stati registrati dall'utente e che quindi non hanno (evidentemente) compromesso l'utilizzazione del servizio. Si tratta evidentemente di previsioni che attenuano la vincolatività degli SLA per il *provider* e la cui ammissibilità per l'utente dovrà essere valutata alla luce del servizio acquisito e dell'attività concretamente svolta dall'utente.
[35] Si pensi, a titolo di esempio, alle condizioni di saturazione della rete pubblica di comunicazioni.
[36] Sul punto si richiama quanto detto *supra* in merito ai rischi di abuso di dipendenza economica, che – secondo la giurisprudenza – può configurarsi anche nel caso di modifiche alle condizioni contrattuali in senso eccessivamente gravoso per la parte che le subisce.
[37] Buttarelli, *Verso un diritto della sicurezza informatica*, in *Riv. Sicurezza e informatica*, Roma, 1995 n.1.
[38] Ai sensi dell'art. 2, lett. a), dir. 95/46/CE, per dato personale deve intendersi *"qualsiasi informazione concernente una persona fisica identificata o identificabile"*, fermo restando che in base al considerando 24 della medesima direttiva *"la presente direttiva lascia impregiudicate le normative relative alla tutela delle persone giuridiche riguardo al trattamento dei dati che le riguardano"* (la normativa italiana contenuta nel Codice in materia di protezione dei dati personali, decreto legislativo 30 giugno 2003, n. 196, estendeva la tutela della disciplina *privacy* anche alle persone giuridiche, enti ed associazioni, ma tale riferimento è stato

soppresso con l'art. 40, comma 2, lettera a), del decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214). Allo stato, per quanto risulta, in Europa residua la sola legislazione austriaca di recepimento della direttiva 95/46/CE che comprende fra i dati tutelati quelli delle persone fisiche, giuridiche nonché dei gruppi di persone (sul punto, e con notevole approfondimento v. Mula, *Wikileaks e la tutela dei dati personali*, in *Dir. inf*., 2011, pagg. 682 e ss.).

[39] In argomento, e per una approfondita disamina, si veda Mantelero, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, in *Dir. inf*., 2010, pag. 678 e ss.

[40] Secondo la terminologia anglosassone del testo della direttiva 95/46/CE (art. 2, lett. d).

[41] Si tratterà principalmente di dati di soci, dipendenti, *partner* commerciali, fornitori, clienti.

[42] Art. 2, lett. e), dir. 95/46/CE.

[43] Sul punto val la pena rilevare che la qualifica di "titolare" o di "responsabile" non è una scelta delle parti (che, ad esempio, pattuiscano nel contratto una determinata ripartizione dei diritti e degli obblighi), ma discende dalla legge in base al concreto assetto dei rapporti intersoggettivi ed alle modalità con cui avviene il flusso di informazioni interno alle modalità di trattamento. In tal senso si veda Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali, *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, Bruxelles, 16/02/2010, pag. 9 (versione italiana), ove si osserva che *"Un criterio puramente formale non sarebbe sufficiente almeno per due ragioni: in alcuni casi la designazione ufficiale di un responsabile del trattamento – prevista ad esempio per legge, in un contratto o in una notificazione al garante per la protezione dei dati – verrebbe semplicemente a mancare; in altri casi, tale designazione ufficiale potrebbe non rispecchiare la realtà, conferendo il ruolo di responsabile del trattamento a un organismo che di fatto non è nella posizione di 'determinare'"*

[44] È stato tuttavia correttamente osservato che, in concreto, il *cloud service provider* si limita (per lo più) a gestire le informazioni ai fini di una elaborazione nell'interesse del proprio cliente così che appaiono ridotti i margini di libertà che potrebbero preludere al riconoscimento della qualità di titolare autonomo o di contitolare. Del resto, come rilevato dal Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali, nel *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, cit., la semplice determinazione degli strumenti tecnici del trattamento da parte del *provider* non fa scattare automaticamente la titolarità autonoma o la contitolarità e ciò in quanto *"la determinazione dei mezzi implicherebbe una responsabilità solo qualora riguardi gli aspetti fondamentali dei mezzi"* (pag. 14).

[45] V. art. 17, dir. 95/46/CE.

[46] Per un inquadramento delle implicazioni del trasferimento dei dati all'estero, si veda Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pagg. 282 e ss.
[47] Questo può dipendere dalla infrastruttura complessa del *provider* e dalle stesse procedure di gestione dei dati implementate da quest'ultimo al fine di garantire funzionalità come *back-up*, scalabilità, ecc.
[48] Sui profili della *due diligence* v. Marchini, *Cloud Computing: a Practical Introduction to the Legal Issues*, London, 2010, pag. 24 e ss.; l'autore evidenzia come nel corso della *due diligence* il *provider* potrebbe esser portato a rivelare informazioni riservate e ciò naturalmente dovrà preferibilmente accadere nel quadro di idonei impegni di riservatezza.
[49] È tuttavia improbabile (per importante che sia il cliente e per elevato che sia il suo potere negoziale) che il *cloud service provider* sia disponibile a recepire puntualmente la propria *security policy*. Infatti, considerata l'architettura *multi-tenanted* del *cloud provider*, è assai difficile – se non impossibile – per quest'ultimo definire una specifica politica di sicurezza per ciascun cliente, poiché essa si rifletterebbe ineludibilmente su altri utenti.
[50] Sarà cura del cliente tenere debita traccia di tali documenti che potranno essere poi allegati al contratto a fini di maggior chiarezza.
[51] Sul punto occorre evidenziare che, ancorché gli *standard* citati riguardino espressamente la gestione della sicurezza delle informazioni e dei dati, essi possono coprire vari aspetti dell'organizzazione del soggetto certificato o che comunque ne assicura il rispetto. L'utente, quindi, dovrà verificare (se del caso chiedendo al *provider* tutta la documentazione a supporto) che le azioni previste dagli *standard* in parola si applichino effettivamente alla soluzione *cloud* cui è interessato. In ottica parzialmente simile, molta attenzione dovrà invece prestare l'utente rispetto alla certificazione SAS 70 vantata da alcuni *cloud provider*. SAS 70, infatti, non è di per sé uno standard tecnologico o di sicurezza, ma uno *standard* per la valutazione, per lo più a fini contabili e finanziari, dei controlli interni delle aziende (specie quelle che offrono attività di *outsourcing*); per tale ragione l'utente interessato ad acquisire i servizi di un *provider* che afferma di essere SAS 70 *compliant* dovrà preferibilmente approfondire il punto chiedendo al *provider* tutta la documentazione di controllo relativa (*report* degli *auditors* indipendenti) ed esaminando attentamente i controlli previsti dal modello.
[52] L'invio dei dati in Paesi in cui il livello di protezione è più basso di quello sancito dalla disciplina comunitaria è *"potenzialmente rischioso per la tenuta dell'intero sistema delle garanzie definite in materia"* (così Mantelero, *Processi di outsourcing*, *cit*., pag. 688). Per comprendere come mai il rischio non riguardi solo il trasferimento verso i Paesi meno sviluppati o con un *deficit* di democrazia, si veda il confronto fra modello

europeo e nordamericano in Mantelero, *Privacy digitale*, *cit.*, pagg. 162 e ss.
[53] Art. 25, co. 1, dir. 96/46/CE. È stato però correttamente osservato (Mantelero, *Processi di outsourcing*, *cit.*, pag. 688) che la direttiva (v. considerando 46 e art. 26, quest'ultimo attuato in Italia dall'art. 43 del Codice Privacy) prevede numerose eccezioni al generale divieto di trasferimento all'estero dei dati, fra cui alcune particolarmente significative se valutate nel quadro di un contratto di servizi cloud: il trasferimento è infatti possibile quando sia stato prestato un preventivo consenso dall'interessato oppure quando è necessario per il perseguimento di finalità contrattuali.
[54] Il giudizio di adeguatezza che permette il trasferimento all'estero dei dati è emesso dal Garante del Paese da cui i dati provengono, anche sulla base di decisioni assunte dalla Commissione Europea ai sensi degli artt. 25, co. 6 e 26, co. 4 della dir. 95/46/CE e con cui la Commissione accerta che un Paese extra UE assicura uno *standard* legislativo di protezione adeguato. Il procedimento – per quanto riguarda il diritto italiano – è regolato dall'art. 44, co. 1, lett. b) del Codice Privacy. Per un elenco aggiornato dei Paesi e per un dettaglio sulle specifiche decisioni si veda http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.
[55] I principi Safe Harbor sono stati approvati dalla Commissione europea con la decisione del 26 luglio 2000, n. 2000/520/CE (i provvedimenti rilevanti sono disponibili in http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm). Essi hanno l'obiettivo di garantire un adeguato trattamento dei dati personali provenienti dall'Europa. Le leggi e la prassi statunitensi in materia di *privacy* e *data protection*, infatti, sono ispirate a principi radicalmente diversi da quelli enunciati dalla direttiva 95/46/CE (sul punto v. Mantelero, *privacy* digitale, *cit.*) e questo disallineamento avrebbe potuto cagionare un problema insormontabile nella cooperazione commerciale ed industriale fra soggetti ed imprese del Vecchio Continente e quelle degli Stati Uniti. I principi *Safe Harbor* non sono immediatamente precettivi per le imprese statunitensi, ma lo diventano una volta che queste vi prestino adesione (è un esempio tipico di *soft law*, strumento assai utile nell'armonizzazione di un settore alquanto magmatico ed in evoluzione come la disciplina della *privacy*) e la vigilanza sull'osservanza degli stessi spetta alla *Federal Trade Commission*. Deve segnalarsi che, recentemente, le Autorità per la protezione dei dati personali dei vari Lander della Repubblica Federale Tedesca hanno deciso che la semplice appartenenza di un'impresa USA alla lista di quelle aderenti al *Safe Harbor* non esime l'esportatore di dati dal verificare concretamente che l'impresa ricevente assicuri un grado di tutela adeguato (decisione del 28/29 aprile 2010 del *Düsseldorfer Kreis*, gruppo di lavoro congiunto delle Autorità per la protezione dei dati personali tedesche). In base a questa decisione, che di

fatto apporta un *vulnus* non da poco alla tenuta del *Safe Harbor*, gli esportatori di dati tedeschi dovranno comunque effettuare dei controlli minimi al fine di verificare che l'importatore dei dati applichi concretamente i principi *Safe Harbor*, restando in caso contrario responsabili in proprio qualora emerga che la condotta dell'importatore non sia nei fatti in linea con i principi *Safe Harbor*.
[56] Art. 44, co. 1, lett. a) come modificata dall'art. 29, comma 5-bis, del decreto legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133.
[57] Art. 44, co. 1, lett. a), Codice Privacy.
[58] Sulle BCR si veda Finocchiaro, *op. cit.*, pagg. 287 e ss.
[59] Si veda in particolare la Decisione della Commissione del 5 febbraio 2010, C(2010)593. Queste clausole, se inserite nel contratto che preveda il trasferimento di dati all'estero, rendono il trasferimento conforme al diritto comunitario. Occorre tuttavia che le parti (in specie l'utente del servizio *cloud*, in quanto esportatore) sia conscio della responsabilità che assume nei confronti degli interessati.
[60] Anche sotto forma di *class action*.
[61] Per inciso, la possibilità per l'importatore di concludere contratti con un subincaricato è soggetto, in base alla clausola 11, al consenso dell'interessato.
[62] Si veda quanto osservato dal Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali, *Parere 3/2009 sulla proposta di decisione della Commissione 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*, Bruxelles, 5 marzo 2009.
[63] Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali, *FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC*, Bruxelles, 12 luglio 2010.
[64] Utilizzatore del servizio *cloud*.
[65] In tal caso l'incaricato diviene l'esportatore ed il subincaricato l'importatore.
[66] È sottinteso che le riflessioni svolte in precedenza sulle clausole di esonero dalla responsabilità devono intendersi generali e comuni ai vari profili di responsabilità contrattuale del *cloud service provider* oggetto della presente relazione.
[67] Di seguito verrà offerta una distinzione fra le informazioni dell'impresa come bene aziendale in senso proprio o come oggetto di protezione di un diritto alla riservatezza analogo a quello delle persone fisiche.

[68] Sul punto si veda, più nel dettaglio, Mantelero, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, *cit.*, pagg. 691 e ss.
[69] È evidente che il rischio di intrusioni esterne (al solo scopo di recar danno ovvero per impadronirsi dei dati) è direttamente proporzionale al sorgere di grandi aggregazioni di dati che tipicamente si verifica presso i *cloud service provider*. In ogni caso si è osservato da più parti che, per la medesima ragione, un *cloud provider* serio attua degli *standard* di protezione mediamente più elevati di quelli di cui un singolo utente potrebbe giovarsi autonomamente.
[70] Art. 98, Decreto legislativo 10 febbraio 2005, n. 30 (Codice della proprietà industriale). La norma rafforza notevolmente la protezione (relativa e contro gli atti di concorrenza sleale) già accordata alle informazioni aziendali riservate dall'art. 6-*bis* del Regio decreto 29 giugno 1939, n. 1127 (legge invenzioni). Gli elementi costitutivi della fattispecie sono esattamente quelli contemplati dall'art. 39 dell'Accordo TRIPs (*Agreement on Trade-Related Aspects of Intellectual Property Rights*, firmato a Marrakesh, Marocco, il 15 aprile 1994 nel quadro dell'Uruguay Round), che costituisce la matrice internazionale della norma interna e di quelle, analoghe, adottate da svariati Paesi.
[71] La norma recita precisamente *"nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore"*. Si tratta di un concetto di segretezza non assoluto: le informazioni si considerano segrete non solo quando sono note esclusivamente ad un imprenditore, trovandosi gli altri nell'impossibilità di apprenderle se non attraverso un negozio di cessione o licenza, ma anche quando, pur essendo conosciute a più operatori del settore (da determinarsi in base all'ambito economico e territoriale di operatività dell'impresa) il loro grado di diffusione è comunque talmente basso da considerarle difficilmente accessibili ai terzi esperti. Sono quindi considerate informazioni non segrete, ai sensi della norma in esame, quelle che possono essere apprese concretamente da ciascuna impresa, in tempi e a costi ragionevoli. In tal senso v. Franchini Stufler, *Il know-how e la tutela dei segreti d'impresa*, Milano, 2009, pagg. 101 e ss.; MANSANI, *La nozione di segreto di cui all'art. 6-bis l.i.*, in *Il dir. ind.*, 2002, pp. 217 ss.
[72] Il valore economico delle informazioni in questione deve derivare dal carattere segreto delle stesse nel senso che se divenissero di pubblico dominio le caratteristiche intrinseche delle medesime non sarebbero sufficienti a conservare il loro valore patrimoniale per l'impresa detentrice. Sul punto v. Franchini Stufler, *op. cit.*, pagg. 104 e ss.
[73] Sono tutelate dalla norma in esame quelle conoscenze che non solo siano attualmente segrete, ma siano altresì sottoposte a misure adeguate a conservare tale carattere nel tempo. L'imprenditore dovrà quindi, da un

lato adottare misure volte ad impedire concretamente a terzi non autorizzati l'accesso alle informazioni riservate e dall'altro lato manifestare a dipendenti, collaboratori e *partner* commerciali la volontà di mantenerle segrete, con obblighi precettivi di questi ultimi. Sul punto osserva Mansani, *op. ult. cit.*, che le misure di sicurezza devono essere coercibili: *"non si può cioè richiedere all'imprenditore di adottare ogni misura disponibile o di fare ogni sforzo possibile per impedire che le informazioni perdano il carattere di segretezza; occorrerà invece che siano adottati controlli legittimamente esigibili dall'imprenditore. (...) Oltre all'esigibilità dei controlli si richiede anche un'esigibilità dei costi"*. Cfr. Franchini Stufler, *op. cit.*, pagg. 100 e ss.

[74] Colangelo, *Diritto comparato della proprietà intellettuale*, Bologna, 2011, pag. 270.

[75] L'impresa che vede irrimediabilmente leso il diritto assoluto sui propri dati aziendali, infatti, perde di norma anche la posizione di vantaggio concorrenziale che il possesso ed uso esclusivo di tali dati comporta.

[76] V. *supra* nota 37. Per un inquadramento, anche in chiave comparatistica, del tema della *privacy* delle persone giuridiche si veda Mula, *Wikileaks e la tutela dei dati personali*, *cit.*, pagg. 682 e ss.

[77] Mula, *Wikileaks e la tutela dei dati personali*, *cit.*, pag. 683. L'Autore sottolinea come tale diritto non sarebbe una sommatoria dei diritti dei singoli membri della collettività, ma un diritto parzialmente autonomo.

[78] Bradshaw, Millar e Walden, *op. cit.*, pagg. 21-22.

[79] Per maggiori dettagli sul *leading case* v. Visintini, Trattato della responsabilità contrattuale vol. 3 - Il risarcimento del danno contrattuale. La responsabilità per ritardo e per fatto degli ausiliari, Padova, 2009, pagg. 383 e ss.

[80] Convenzione delle Nazioni Unite sui Contratti di Compravendita Internazionale di Merci, adottata a Vienna l'11 aprile 1980, ratificata dall'Italia con Legge 11 dicembre 1985, n. 765.

[81] Art. 7.4.2.

[82] Art. 7.4.4.

QUADERNI DI
DIRITTO MERCATO TECNOLOGIA
Numero 1 - 2013
Anno III
www.dimt.it
ISSN (Online edition): 2239-7442