ALESSANDRO MANTELERO

PROCESSI DI *OUTSOURCING* INFORMATICO E *CLOUD COMPUTING*: LA GESTIONE DEI DATI PERSONALI ED AZIENDALI

SOMMARIO: 1. La rilevanza socio-economica e la natura giuridica dei processi di *outsourcing*. — 2. Il *cloud computing* ed il trattamento dei dati personali: l'organigramma del trattamento. — 3. (*Segue*): le implicazioni correlate alla connotazione transfrontaliera del trattamento. — 4. La sicurezza dei dati e delle informazioni aziendali.

1. La rilevanza socio-economica e la natura giuridica dei processi di *outsourcing*.

Il *cloud computing*[1] consiste in un insieme di tecnologie e risorse informatiche, accessibili direttamente *on-line* grazie allo sviluppo delle reti di comunicazione[2], autonomamente predisposto e controllato dall'impresa ovvero alla stessa fornito da terzi sotto forma di servizio[3].

La scelta di affidarsi a prodotti commerciali sembra essere quella preferita dal crescente numero di realtà produttive che sta migrando verso questa nuova tipologia di soluzioni e pare, anche in prospettiva, quella destinata a prevalere, benché ad oggi le aziende di maggiori dimensioni sovente preferiscano la modalità *in house* per i propri servizi *cloud*. Per tale ragione, tenuto altresì

[1] Per un'analisi tecnico-informatica dei sistemi di *cloud computing*, delle loro architetture e del loro funzionamento, cfr. Sun Microsystems, *Introduction to Cloud Computing Architecture. White Paper*, 1st Edition, giugno 2009, in *http://webobjects.cdw.com/webobjects/media/pdf/Sun_CloudComputing.pdf*. Per uno studio che tiene conto anche delle dinamiche economiche, si veda inoltre Aa.Vv., *Above the Clouds: A Berkeley View of Cloud Computing*, 10 febbraio 2009, in *http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html*. Cfr. inoltre Expert Group Report, *The Future Of Cloud Computing*, rapporto redatto per la Commissione europea, 2010, in *http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf* (tutte le risorse *on-line* citate nel presente contributo sono state consultate fra il 3 giugno 2010 ed il 3 agosto 2010).

[2] Per una definizione di dettaglio cfr. P. Mell-T. Grance, *The NIST Definition of Cloud Computing*, version 15, 7 ottobre 2009, in *http://csrc.nist.gov/groups/SNS/cloud-computing/*.

[3] L'idea dell'informatica come servizio, anziché come bene, è risalente nella sua elaborazione teorica, cfr. D.F. Parkhill, *The Challenge of the Computer Utility*, Reading (Mass.), 1966.

conto di come la realizzazione autonoma del *cloud* da parte dell'impresa semplifichi alquanto il modello (per l'accentramento organizzativo e di gestione dei dati che in tal modo si realizza), il contesto di analisi maggiormente interessante, per varietà di rapporti giuridici, appare quello in cui vengono a coesistere tanto le componenti informatiche correlate al *cloud computing* quanto i processi di *outsourcing*, cui pertanto sarà rivolta la presente indagine.

Come è noto con il termine *outsourcing*, in un'ottica aziendalista[4], si intende quel processo in virtù del quale alcune attività proprie di un'impresa vengono affidate a terzi ed in tal modo portate al di fuori dell'azienda, attraverso un mutamento strutturale con evidenti implicazioni organizzative e strategiche in termini di gestione e controllo dei processi e delle informazioni, nonché di passaggio da un controllo diretto ed interno ad un modello governato in prevalenza mediante il ricorso a strumenti contrattuali[5].

Varie e contingenti le ragioni che inducono a porre in essere tali operazioni di riorganizzazione, che muovono tuttavia da due istanze principali: la necessità per l'impresa di investire sul proprio *core business* e la riduzione dei costi. Quanto al primo aspetto, l'attribuzione a soggetti esterni delle attività ripetitive ed a basso valore aggiunto, o di quelle ritenute comunque non strategiche, consente di recuperare risorse da destinare ai rami più profittevoli, potendo comunque continuare a fruire dei risultati di tali attività, ricevendoli dagli *outsourcee* sotto forma di prestazioni di servizi. Nel contempo l'attribuzione di tali compiti a realtà aziendali che incentrano il loro *business* proprio su tali processi o servizi permette a quest'ultime di conseguire economie di scala, con una riduzione di costi che si traduce, in ultima analisi, in un contenimento del prezzo che l'*outsourcer* viene a pagare per fruire dei servizi esternalizzati, con un costo inferiore a quello della gestione *in house*.

I vantaggi dell'*outsourcing* emergono poi sotto un ulteriore profilo, che assume connotazione rilevante nell'ambito dell'*information and communication technology* (ICT): la gestione del rischio. La centralità vitale dei servizi informatici per il funzionamento di un'azienda è infatti tale per cui qualsiasi interruzione o anche solo

---

[4] Per eventuali approfondimenti nella letteratura aziendalistica, cfr., senza pretesa di completezza: R.H. Coase, *The nature of the firm*, in *Economica*, vol. 4, no. 16, 1937, 386 ss.; O.E. Williamson, *Markets and Hierarchies; Analysis and Anti-Trust Implications*, New York, 1975; U. Arnold, *New dimensions of outsourcing: a combination of transaction cost economics and the core competencies concept*, in *European Journal of Purchasing & Supply Management*, n. 6 (1), 2000, 23 ss.

[5] È questo il modello di *outsourcing* (c.d. *direct third party outsourcing*) che qui interessa, poiché ad esso fanno principalmente riferimento le operazioni che vedono il ricorso al *cloud computing*, mentre non verranno considerati i diversi modelli in cui si prevede la creazione di un'unità operativa all'estero da parte di una società madre (*captive direct*) o in cui si dà vita ad una *joint venture* con la società estera *outsourcee*.

rallentamento del loro funzionamento si traduce immediatamente in oneri aggiuntivi, ne consegue che il rischio informatico (dai guasti dell'*hardware*, ai *bug* dei sistemi, agli attacchi esterni) comporta necessariamente l'adozione di tutta una serie di misure di prevenzione, nonché il pronto intervento qualora esso si concretizzi. A tal fine occorre impiegare notevoli risorse finanziarie nonché un congruo numero di dipendenti, spesso di elevata qualifica tecnica, a fronte di un rischio la cui potenzialità non è in ogni caso nota *a priori* e per questo di non facile stima in termini esatti di costo, con difficoltà di gestione finanziaria dello stesso. In quest'ottica l'attribuzione a terzi delle competenze informatiche implica anche un'esternalizzazione delle relative attività di prevenzione, *business continuity* e *disaster recovery*, consentendo in tal modo di conseguire altresì una maggior certezza dei costi associati, in parte traslati sull'*outsourcee* (manutenzione ecc.), in parte ad esso attribuibili in via contrattuale, in quanto riconducibili a forme di inadempimento (ad esempio attraverso quantificazione preventiva con clausola penale del danno stimato in caso di interruzione temporanea del servizio), potendo eventualmente ricorrere al sistema assicurativo in via integrativa[6].

Coerenti con tali istanze risultano le motivazioni che stanno spingendo diverse aziende a realizzare processi di *outsourcing* informatico avvalendosi della tecnologia del *cloud computing*. Sfruttando le potenzialità della comunicazione attraverso reti telematiche è infatti possibile concentrare in grandi *data center* le risorse informatiche di più aziende, che accederanno ad esse per compiere le usuali operazioni di elaborazione dati[7]. I gestori di tali

[6] Cfr. in generale sul ricorso allo strumento assicurativo in relazione al rischio informatico: E. NASTRI, *Verso una polizza assicurativa dei rischi informatici*, in questa *Rivista*, 1989, 981 ss.; S. TRAVERSO, *Assicurazione e* software, *ivi*, 1987, 312 ss.; F. STORACE, *La copertura assicurativa del « rischio informatico »*, *ivi*, 1986, 652 ss.; V. ZENO-ZENCOVICH, *Sul rilievo pratico e sistematico della categoria dei c.d. contratti di informatica*, in *I contratti di informatica. Profili civilistici, tributari e di bilancio*, a cura di G. Alpa-V. Zeno-Zencovich, Milano, 1987, 40 s.; G.B. FORLINO, *Assicurazione e diritto informatico: i contratti assicurativi di base*, *ivi*, 361 ss.

[7] Va in proposito notato come il *cloud computing* costituisca un'epifania del processo in corso da diversi anni in virtù del quale si assiste ad uno spostamento dalle tradizionali logiche proprietarie a quelle contrattuali, incentrate sul servizio, cfr. a riguardo J. RIFKIN, *L'era dell'accesso*, Milano, 2000, 117: « dotati di un contenuto di informazione sempre più determinante, di una maggiore interattività, ed essendo sottoposti a continui miglioramenti, i beni cambiano carattere. Perdono il proprio status di prodotti e acquisiscono quello di servizi in evoluzione ». Nello specifico la fruizione di *data center*, ma anche l'utilizzo di *software* ed ambienti di sviluppo, direttamente *on-line*, esclude la necessità di acquistare beni, godendone comunque sotto forma di servizio; cfr. SUN MICROSYSTEMS, *Introduction to Cloud Computing Architecture. White Paper*, citato *supra*, 1: « What distinguishes cloud computing from previous models? Boiled down to a phrase, it's using information technology as a service over the network ». Cfr. anche INTERNATIONAL TELECOMMUNICATION UNION, *Distributed Computing: Utilities, Grid & Clouds*, 2009, 1, in *www.itu.int/oth/T2301000009/en*, in cui si sottolinea come « a new paradigm is emerging in which computing is offered as a utility by third parties whereby the user is billed only for consumption ».

centri possono poi anche fornire all'utenza servizi ulteriori rispetto al semplice *storage* dei dati, dalla fruizione di *software* direttamente operativi *on-line*, agli ambienti di sviluppo e programmazione.

Rinviando al seguente paragrafo per un maggior dettaglio circa la tipologia dei servizi riassuntivamente unificati sotto la definizione di *cloud computing*, è tuttavia sin d'ora evidente come tale tecnologia non faccia che rispondere in maniera più avanzata e soddisfacente alle ragioni sottostanti ai più generali processi di *outsourcing* informatico, ridefinendole e contestualizzandole rispetto al quadro tecnologico attuale che vede un ruolo preponderante attribuito alla comunicazione *on-line*, all'interconnessione permanente fra i dipendenti delle aziende più innovative e fra le stesse ed i rispettivi clienti o fornitori, il tutto acuito dallo sviluppo su scala globale dei rapporti lavorativi e commerciali. A ciò si aggiunga che le soluzioni *cloud* offerte dai diversi operatori possono risultare particolarmente appetibili per le piccole e medie imprese, cui vengono offerti servizi aventi lo *standard* delle grandi imprese, dei quali non potrebbero fruire se dovessero contare solamente sulle proprie risorse *in house*, ma di cui hanno necessità per competere sul mercato globale.

Sotto il profilo dei costi va inoltre tenuto conto come nel mondo più industrializzato quelli energetici (energia elettrica), nonché quelli attinenti il godimento degli immobili (i *data center* necessitano infatti di locali *ad hoc*) e quelli del lavoro permangano significativi, da qui il vantaggio nella delocalizzazione laddove questi oneri risultino minori, senza che ciò, in ragione della concomitante diminuzione dei costi di connessione telematica, comporti particolari oneri aggiuntivi.

Alle ragioni già individuate come influenti sulle scelte aziendali di esternalizzazione (concertazione delle risorse, riduzione di costi, gestione del rischio)[8] si aggiunge poi, nel caso del *cloud computing*, la possibilità di ottimizzare lo sfruttamento della dotazione informatica in termini di pieno utilizzo. Gran parte del potenziale degli elaboratori presenti in un'azienda risulta infatti inutilizzato o sotto-utilizzato in diversi momenti[9], oppure impegnato per l'ope-

---

[8] Cfr. nel dettaglio, in relazione al *cloud computing*: IBM, *Diradare le nebbie attorno al cloud computing*, Segrate, 2010, 5; NextValue, *Cloud computing un anno dopo. CIO italiani e CIO europei a confronto*, Milano, 2010, 28, fig. 12 e 13, 30 s. Con riferimento ai processi di *outsourcing* nel settore ICT in generale, oltre che al *cloud computing*, cfr. anche Politecnico di Milano-Dipartimento di Ingegneria Gestionale, *ICT Strategic Sourcing: nuovi equilibri oltre la crisi. Rapporto 2009 Osservatorio ICT Strategic Sourcing*, novembre 2009, in *http://www.osservatori.net/ict_strategic_sourcing/rapporti/rapporto/journal_content/56_INSTANCE_0HsI/10402/574901*.

[9] Si pensi al lasso di tempo in cui i sistemi non sono utilizzati dagli utenti perché è terminato l'orario di lavoro o ancora alle ipotesi in cui sia necessario disporre di ampie risorse a causa di picchi di lavoro che si presentano solo in alcuni momenti nell'arco temporale. In termini generali si stima

rativ**ità dei *software* o destinato allo *storage*; esternalizzando tali funzioni si vengono a ridurre le risorse necessarie all'*outsourcer*, ottimizzando inoltre quelle di cui si fruisce in modalità *cloud*[10], e nel contempo, in virtù della concentrazione dei servizi offerti a più soggetti, si realizzano economie di scala per l'*outsourcee*, con abbassamento dei costi di servizio nonché, in termini globali, con un minor spreco di risorse energetiche[11].**

Guardando alle ricadute in termini giuridici dei processi ora descritti, esse concernono tanto la regolamentazione contrattuale, mediante la quale l'*outsourcing* si realizza[12], quanto il trattamento dei dati aziendali che quest'ultimo necessariamente comporta.

Nello specifico, l'operazione di *outsourcing* è suscettibile di essere effettuata facendo ricorso alternativamente ad una pluralità di accordi contrattuali, declinata secondo le esigenze delle parti, al fine di disciplinare tanto il conferimento delle attività dall'*outsourcer* all'*outsourcee*, quanto la successiva erogazione delle medesime sotto forma di prestazione dei servizi[13]. Altrettanto complessa è la regolamentazione, sia pattizia che normativa, dei

che l'utilizzo dei *server* dei *data centers* vari fra il 5% ed il 20%; cfr. AA.VV., *Above the Clouds: A Berkeley View of Cloud Computing*, citato *supra*, 10.

[10] I sistemi di *cloud computing* si caratterizzano infatti per la scalabilità, ovvero la flessibilità nell'erogare quantitativamente le risorse informatiche (potenza dei processori, dimensione dell'architettura, ampiezza dello *storage*, ecc.) in ragione delle esigenze contingenti, diversamente da quanto accade per le risorse aziendali che devono essere stimate sui livelli massimi di utilizzo per farvi fronte, sebbene ciò possa comportare un loro diffuso sotto-utilizzo. L'ottimizzazione delle risorse informatiche può dunque avvenire anche attraverso un'integrazione fra quelle aziendali, destinate a sostenere i flussi lavorativi ordinari, con quelle di *cloud computing*, volte a soddisfare quelle eccezionali.

[11] Secondo alcuni operatori, poi, il *cloud computing* potrebbe rivelarsi una soluzione facilitante i processi di fusione/acquisizione fra imprese, semplificando e riducendo i costi di integrazione fra le risorse informatiche.

[12] Va sottolineato come l'*outsourcing* rilevi sotto il profilo funzionale ed organizzativo e non in quanto modello contrattuale o categoria giuridica autonoma, cfr. in tal senso F. CARDARELLI, *La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing*, in questa *Rivista*, 1993, I, 86, secondo cui tale termine « non può avere alcuna rilevanza giuridica »; così anche M. PITTALIS, *Outsourcing*, in *Contr. e impr.*, 2000, 1006 s. Con riguardo al profilo contrattuale inerente la gestione del processo di *outsourcing* informatico si vedano: F. TOSI, *Il contratto di outsourcing di sistema informatico*, Milano, 2001; M. PITTALIS, *op. cit.*, 1010 ss.; A. MUSELLA, *Il contratto di* outsourcing *del sistema informativo*, in questa *Rivista*, 1998, 857 ss.; F. CARDARELLI, *op. cit.*, 85 ss.

[13] Non essendo questa la sede per approfondire gli aspetti contrattuali generali dei processi di *outsourcing*, sia sufficiente rilevare come mentre nel porre in essere l'esternalizzazione solitamente si ricorre ad una varietà di modelli, l'acquisizione del servizio erogato dall'*outsourcee* risulta in genere sussumibile nel contratto di appalto di servizi, cfr. O. CAGNASSO-G. COTTINO, *Contratti commerciali*, in *Trattato di Diritto Commerciale* diretto da G. Cottino, Padova, 2000, 353, secondo cui l'*outsourcing* costituisce spesso un contratto quadro, comprensivo delle varie declinazioni non tipizzate che può assumere la prestazione di servizi informatici; si vedano nello stesso senso: M. PITTALIS, *Outsourcing*, citato *supra*, 1015 s.; A. MUSELLA, *Il contratto di* outsourcing *del sistema informativo*, citato *supra*, 859 ss.; F. CARDARELLI, *La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing*, citato *supra*, 94.

flussi di dati che il processo di *outsourcing* genera in maniera bidirezionale fra le parti. Quest'ultimo aspetto, benché meno indagato, è destinato, sotto il profilo operativo, ad assumere notevole rilievo nei contesti di *outsourcing* informatico ed in quello specifico che si realizza attraverso il *cloud computing*, in ragione della connotazione dei servizi in questione, fisiologicamente destinati al processamento di dati. Per tale motivo l'analisi che si svilupperà nei successivi paragrafi verrà incentrata principalmente sulla gestione delle risorse informative, tenendo conto della duplice rilevanza che possono assumere le informazioni aziendali, in quanto dati personali, tutelati nell'interesse del soggetto cui si riferiscono, ed in quanto informazioni riservate, protette in un'ottica di segreto aziendale. Sotto entrambi i profili, centrali risultano le modalità organizzative adottate dalle parti, in ragione delle conseguenti ricadute in termini di responsabilità, rispetto alle quali ulteriori complessità derivano dagli elementi di internazionalità che solitamente caratterizzano il *cloud computing*.

2. Il *cloud computing* ed il trattamento dei dati personali: l'organigramma del trattamento.

L'intenso flusso di dati che solitamente si genera fra le imprese coinvolte nei processi di *outsourcing* riguarda informazioni che, in molti casi, rivestono la natura di dati personali, in quanto riferite a terze persone direttamente o indirettamente individuabili (dipendenti, fornitori, *partner* commerciali, clienti)[14]. Se è dunque fuor di dubbio che tali operazioni di gestione e (ri)organizzazione aziendale comportino il venir in essere di diversi trattamenti di dati, può invece risultare più controversa la qualificazione giuridica del ruolo assunto dai soggetti che concorrono ad essi e, con-

[14] 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 »; cfr. inoltre 24° considerando, secondo cui « la presente direttiva lascia impregiudicate le normative relative alla tutela delle persone giuridiche riguardo al trattamento dei dati che le riguardano ». Si veda anche Articolo 29 Gruppo di lavoro per la protezione dei dati personali, *Parere 4/2007 sul concetto di dati personali*, Bruxelles, 20 giugno 2007, 22 ss., in *http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2010_en.htm*. Solo alcuni stati (Italia, Austria, Lussemburgo), hanno invece ritenuto di estendere tale nozione anche alle persone giuridiche, con una scelta da ritenersi legittima secondo l'insegnamento della Corte di Giustizia delle Comunità europee che, in una nota pronuncia (sentenza del 6 novembre 2003, C-101/01, caso *Lindqvist*), ha affermato che « nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46 a settori non compresi nell'ambito di applicazione di quest'ultima, purché non vi osti alcun'altra disposizione del diritto comunitario ». Laddove sia stata adottata la nozione più estensiva di dato personale, rientreranno dunque in tale definizione anche le informazioni inerenti le imprese oggetto del processo di *outsourcing*.

seguentemente, la definizione delle specifiche responsabilità e degli obblighi incombenti[15].

In termini generali occorre in primo luogo tener presente che la normativa comunitaria in materia di dati personali ha una struttura dato-centrica, in virtù della quale il ruolo assunto dagli autori del trattamento è determinato in ragione della relazione che ciascuno legittimamente instaura con le informazioni piuttosto che in virtù della natura dei rapporti intersoggettivi. Da ciò consegue che l'organigramma del trattamento dati, incentrato su di una sostanziale tripartizione di figure[16] (« controller », « processor » e « persons who, under the direct authority of the controller or the processor, are authorized to process the data »[17]), non risulta necessariamente sovrapponibile a quello aziendale, né condizionato dall'autonomia soggettiva delle parti contraenti.

Per quanto qui interessa, va in particolare osservato come l'attribuzione di compiti di gestione delle informazioni ad un'altra impresa non comporti necessariamente che dall'esistenza di due entità separate consegua altresì un'autonomia sul piano del trattamento dati, potendo benissimo l'una fungere da *controller* e l'altra da *processor*, al primo correlato e subordinato. La valutazione va infatti condotta in ragione delle differenti posizioni assunte in concreto dai soggetti rispetto al trattamento dati — destinate a prevalere sulla stessa qualificazione convenzionalmente definita dalle parti[18] — ed alla luce del dettato normativo comunitario che qualifica come *controller* la persona fisica o giuridica « which… determines the purposes and means of the processing of personal data »[19] e come *processor* la persona fisica o giuridica « which pro-

[15] Cfr. a riguardo Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, Bruxelles, 16 febbraio 2010, 2, in *http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2010_en.htm*: « The Working Party recognizes that the concrete application of the concepts of data controller and data processor is becoming increasingly complex. This is mostly due to the increasing complexity of the environment in which these concepts are used, and in particular due to a growing tendency, both in the private and in the public sector, towards organisational differentiation, in combination with the development of ICT and globalisation ».

[16] Cfr. art. 2, lett. *d*), *e*) ed *f*), dir. 95/46/CE e, con riguardo alla normativa nazionale art. 4, comma 1, lett. *f*), *g*) e *h*), D.Lgs. 196/2003; dato il carattere sovranazionale dei processi in esame, nel testo — salvo diversa indicazione — si farà riferimento principalmente alle fonti comunitarie.

[17] Corrispondenti, rispettivamente, al titolare, responsabile ed incaricato del trattamento di cui al D.Lgs. 196/2003, cfr. nota precedente.

[18] Cfr. Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 9: « even though the designation of a party as data controller or processor in a contract may reveal relevant information regarding the legal status of this party, such contractual designation is nonetheless not decisive in determining its actual status, which must be based on concrete circumstances ».

[19] Cfr. art. 2, lett. *d*), dir. 95/46/CE, nonché il successivo art. 17. Cfr. inoltre a riguardo, Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 4, secondo cui « first and foremost role of the concept of control-

cesses personal data on behalf of the controller »[20], con l'avvertenza che nel caso di processi di *outsourcing* il *processor* potrebbe essere individuato tanto nella società stessa *outsourcee* (soluzione che pare più agevole), quanto in una persona fisica da essa dipendente o esterna alla medesima, ma contrattualmente incaricata di svolgere tale funzione.

È dunque la sussistenza di un rapporto di preposizione e l'esistenza in capo al preponente del potere decisionale in merito al trattamento, che consente di distinguere i ruoli[21], non la tipologia di relazioni che lega i soggetti sul diverso piano economico-funzionale ed in particolare la qualifica di *outsourcer* od *outsourcee*. Per questo occorrerà verificare il livello di autonomia detenuto da ciascuna parte rispetto alle varie attività comportanti la gestione dei dati[22].

Qualora sussista in capo ad ognuna delle imprese un'ampia libertà decisionale nel definire i caratteri essenziali del trattamento[23] saremo in presenza di due distinti *controller*, con la conseguenza che il flusso di informazioni che si instaurerà fra di essi verrà necessariamente qualificato in termini di trasmissione di dati fra autonomi titolari del trattamento; diversamente, ove la gestione dei dati operato dall'*outsourcee* risulti eterodiretta dall'*outsourcer*[24], ne conseguirà che verrà in essere un rapporto fra *processor* e *controller*, in ragione del quale lo scambio di dati potrà essere più semplicemente ricondotto ad un flusso di informazioni interno alle modalità di trattamento.

---

ler is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice ». Nel caso di realtà societarie è ritenuto preferibile individuare il *controller* nella persona giuridica anziché in singoli dipendenti della stessa, cfr. in tal senso Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, *cit.*, 15.

[20] Cfr. art. 2, lett. *e*), dir. 95/46/CE.

[21] Cfr. in tal senso Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 4 e 9.

[22] Un'espressa indicazione nel senso di operare una qualificazione giuridica dei soggetti, ai fini del trattamento, in ragione dell'effettivo potere di determinarne le modalità, desumibile dagli elementi fattuali e dalle circostanze concrete, emerge in Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 8, ove si sottolinea altresì come « a merely formal criterion would not be sufficient… it may happen that the formal appointment would not reflect the reality, by formally entrusting the role of controller to a body which actually is not in the position to ''determine'' ».

[23] Al riguardo possono anche assumere rilievo le specifiche competenze professionali del destinatario dei dati, che, ove rivestano un ruolo determinante ai fini del trattamento da quest'ultimo posto in essere, possono costituire un'ulteriore indice nel senso della qualificazione dello stesso quale *controller*; cfr. Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 28.

[24] Nello specifico occorre però che non ci si limiti a « very general instructions », indicando solamente il genere di servizio richiesto, ma occorre che quest'ultimo sia regolato in un maggior dettaglio, altrimenti prevarrebbe l'autonomia decisionale dell'*outsourcee* con conseguente qualifica dello stesso quale *controller*; cfr. Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 29.

Rilevanti le implicazioni correlate all'adozione dell'uno o dell'altro modello organizzativo, incidenti tanto sul profilo gestionale che su quello della responsabilità, tali da comportare vantaggi e svantaggi per molti versi speculari rispetto alle due soluzioni ipotizzabili.

Se infatti viene privilegiata l'indipendenza dei soggetti, l'*outsourcer* beneficerà di una riduzione degli oneri in termini di adempimenti normativi, in relazione ai trattamenti esternalizzati, così come non potrà essere ritenuto responsabile per gli illeciti posti in essere dal destinatario delle informazioni. A riguardo va tuttavia considerato il problema dei possibili danni « indiretti » causati dall'illecito trattamento (danno di immagine e perdita della clientela potenziale futura, ad esempio) conseguenti ai comportamenti tenuti dall'*outsourcee* nella gestione dei dati. In proposito, al di là dell'esercizio in giudizio di un'azione risarcitoria verso la controparte, l'*outsourcer* potrebbe regolamentare più efficacemente tale aspetto in via preventiva attraverso l'adozione di apposite clausole contrattuali che tengano conto di queste eventualità e, integrando sul punto il regolamento dell'operazione di *outsourcing*, vadano a quantificare preventivamente i danni e/o a prevedere specifiche ipotesi di risoluzione del contratto[25].

Per converso un modello analogo a quello ora considerato fa venir meno, con riguardo al trattamento dati, il controllo dell'*outsourcer* sull'attività dell'*outsourcee*, e rende inoltre opportuna una programmazione *ad hoc* sin dall'origine. In ragione del principio di pertinenza[26] e del consenso prestato dall'interessato sulla base di una precisa informativa in cui vengono esplicitate le finalità specifiche dal trattamento[27], qualora si ritenga di comunicare a terzi (in questo caso all'*outsourcee*) i dati raccolti è infatti necessario farne dapprima menzione nell'informativa[28] e successivamente acquisire il consenso degli interessati anche a tal fine[29]. In assenza dell'assolvimento preventivo a tali adempimenti la comunicazione sarà possibile solamente al prezzo di fornire in un secondo momento opportuna informativa agli interessati e richie-

[25] Con riferimento in generale all'inadempimento nei contratti mediante i quali si realizza il processo di *outsourcing* cfr. A. Zincone, *Il contratto di outsourcing: natura, caratteristiche, effetti*, in *Dir. aut.*, 2002, 398 ss., che sottolinea come, in ragione della complessità degli interessi in gioco e del rapporto di interdipendenza che si crea fra *outsourcer* ed *outsourcee*, sia preferibile superare le eventuali patologie dell'esecuzione ricorrendo a soluzioni negoziali e conciliative.

[26] Cfr. art. 6, paragrafo 1, lett. *c*), dir. 95/46/CE, cui corrisponde l'art. 11, comma 1, lett. *d*), D.Lgs. 196/2003.

[27] Cfr. artt. 6, paragrafo 1, lett. *b*), 7, lett. *a*) e 10, lett. *b*), dir. 95/46/CE; per la normativa italiana il riferimento principale è invece l'art. 23, comma 3, D.Lgs. 196/2003.

[28] Cfr. art. 10, lett. *c*), dir. 95/46/CE, nonché art. 13, comma 1, lett. *d*), D.Lgs. 196/2003.

[29] Con riguardo al requisito del consenso occorrerà tener conto delle ipotesi in cui l'acquisizione dello stesso risulti però superflua ai sensi dell'art. 7, dir. 95/46/CE.

derne specificatamente il consenso, con ovvi oneri aggiuntivi e con il rischio che solo una parte degli interpellati esprima la propria volontà.

Nel caso in cui l'*outsourcee*, sotto il profilo del trattamento dati, venga invece assorbito nella sfera organizzativa e di controllo dell'*outsourcer*, rivestendo conseguentemente la qualifica di *processor*, le posizioni di vantaggio e svantaggio risulteranno nella sostanza invertite rispetto al caso precedente. L'*outsourcer* avrà così da un lato un completo controllo sulla gestione dati e non dovrà porre in essere particolari adempimenti formali nei confronti degli interessati, in termini di informativa ed acquisizione del consenso specifico, ma d'altro canto da tali maggiori poteri conseguirà necessariamente la responsabilità in ordine agli aspetti organizzativo-gestionali allo stesso ascritti dalla normativa, all'onere di predisporre l'adozione delle misure di sicurezza e vigilare sulla loro applicazione, nonché alla scelta del soggetto designato quale *processor*, di cui occorrerebbe accertare preventivamente i requisiti di affidabilità e competenza previsti dall'art. 17, paragrafo 2, della direttiva 95/46/CE[30].

Al fine di trasporre le considerazioni ora formulate nello specifico contesto del *cloud computing*, occorre in primo luogo definire nel dettaglio le applicazioni concrete di questa soluzione tecnologica, distinguendo tra i diversi servizi erogati mediante tale modalità, in ragione della necessità di guardare al dato fattuale al fine di delineare i rapporti fra i soggetti agenti rispetto alla gestione dei dati.

Tre sono a riguardo le tipologie rinvenibili, tutte accomunate dallo spostamento delle risorse informatiche impiegate dalla macchina dell'utente o dai *server* aziendali ad uno o più *data center* accessibili mediante reti di telecomunicazione:

— *cloud software as a service (SaaS)*, in cui all'utente viene data la possibilità di fruire in remoto di applicativi *software* offerti da terze parti (es. servizi di posta elettronica accessibili da interfaccia web, come AOL), senza però gestirne i profili operativi in termini di impiego delle risorse informatiche (infrastrutture, sistemi operativi, *storage*, ecc.), salvo alcune limitate personalizzazioni del servizio;

— *cloud platform as a service (PaaS)*, in cui all'utente viene offerto non un *software*, ma un'intera piattaforma, composta di

[30] Quest'ultimo profilo costituisce un punto non secondario all'interno dell'organizzazione aziendale e, più in generale, nei processi di *outsourcing*, laddove sovente le competenze in materia di trattamento dati vengono affidate a dirigenti apicali quando non addirittura alla persona giuridica nel suo complesso (questo nel caso di società controllate/collegate o di *outsourcing*), apparentemente seguendo criteri squisitamente organizzativi, a prescindere da un effettivo vaglio della sussistenza dei criteri qualitativi richiesti.

diversi servizi e programmi, entro la quale possono essere sviluppati applicativi creati dallo stesso utente o da questi acquisiti[31];

— *cloud infrastructure as a service (IaaS)*, in cui all'utente vengono fornite risorse *hardware* altrui da gestire in remoto e su cui installare e far funzionare i propri sistemi operativi ed i propri *software*[32], con il vantaggio di un accesso ubiquo, ovvero da qualsiasi luogo in cui si possa attivare un'adeguata connessione telematica.

Mediante tali soluzioni[33] viene così generato un insieme eterogeneo e distribuito di risorse fruibile *on-line*, immaginato figurativamente come una « nuvola » (da qui il termine *cloud computing*), come un luogo distaccato da quello in cui risiedono le proprie risorse informatiche materiali. Non solo, sovente il gestore del *cloud* dispone di più *data center* dedicati ai servizi erogati, con la conseguenza che, al fine di saturarne l'utilizzo, le informazioni possono essere spostate da uno all'altro senza che l'utente se ne avveda[34]; tale mobilità può tuttavia comportare l'impossibilità di sapere esattamente dove si trovino localizzate in un dato momento le informazioni residenti all'interno della « nuvola ».

Rispetto al contesto così delineato, interrogandosi sulla qualificazione giuridica del fornitore dei servizi, in ragione della natura e delle modalità con cui la prestazione è offerta, va tenuto conto di come, alla luce delle indicazioni comunitarie[35], anche allorquando il fornitore del servizio mantenga un certo margine di autonomia decisionale ed operativa, laddove i compiti di quest'ultimo vengano « chiaramente e rigorosamente definiti », si deve ritenere che lo stesso non possa essere considerato un *controller*, ma solamente un *processor*. È stato inoltre sottolineato come ove uno solo sia il soggetto direttamente legittimato dagli interessati a trattare i

[31] In tal caso l'utente non ha il controllo della struttura *cloud* (infrastrutture, *server*, sistemi operativi ecc.), ma è in grado di controllare le applicazioni da lui create e configurare l'ambiente di sviluppo. Diversamente può esservi l'ipotesi in cui venga fornita all'utente un'intera piattaforma *hardware* e *software* pre-configurata (es. Microsoft Windows Azure Platform Appliance) da gestire direttamente presso le proprie sedi o *data center*, in questo caso tuttavia non si ha una forma di *outsourcing* fra l'utente ed il fornitore della piattaforma, trattandosi di una struttura *cloud computing* privata gestita dal primo in autonomia, ragion per cui non verrà qui presa in esame.

[32] Nel caso di specie, a differenza di quanto può accadere nel partizionamento delle risorse informatiche all'interno di un ambito aziendale, le risorse vengono assegnate dal gestore del servizio non in maniera statica e definita *a priori*, ma in ragione dell'effettivo utilizzo al momento del bisogno.

[33] Le diverse forme che assume il *cloud computing* sono state qui descritte individualmente, ma è ovviamente possibile che il fornitore del servizio, specie se di maggiori dimensioni, offra un servizio integrato di *cloud computing*, completo in tutti i suoi aspetti, così come è possibile che più fornitori concorrano insieme per dar vita all'intero servizio.

[34] L'utente accede infatti al servizio *cloud* ed è quest'ultimo a reperire e riaggregare le informazioni, che dunque compaiono sull'interfaccia utente nella stessa maniera a prescindere dalla loro localizzazione.

[35] Cfr. Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 13.

dati ed i terzi destinatari delle informazioni abbiano la facoltà di gestirle unicamente in quanto pongano in essere un'elaborazione nell'interesse del primo, si dovrebbe ravvisare un rapporto fra *controller* e *processor*. Tali indicazioni, unitamente alle modalità contrattuali tipiche dell'*outsourcing* in generale e nello specifico dei servizi di *cloud computing*, laddove ampia rilevanza è data alla definizione delle prestazioni ed ai *service level agreement* (SLA)[36], paiono ridurre i margini alla possibile qualificazione dei flussi informativi fra *outsourcer* ed *outsourcee* in termini di rapporto fra autonomi titolari o con-titolari[37].

Guardando poi a ciascuna delle tipologie di *cloud computing* esistenti (SaaS, IaaS e PaaS), si può osservare come nel caso del *software as a service* (SaaS) vi siano tre diverse fasi di trattamento: immissione dei dati avvalendosi dell'interfaccia *software*, elaborazione degli stessi ad opera del *software*, gestione dei dati elaborati (archiviazione, copiatura, *back up*, invio a terzi, ecc.). Occorre dunque distinguere fra quella che è l'elaborazione posta in essere direttamente dal *software* e gli effetti della stessa sulle risorse informatiche rese disponibili dal servizio *cloud*, poiché solamente quest'ultimi configurano operazioni di trattamento da parte del fornitore del servizio[38]. In ultima analisi dunque fulcro dell'attività di gestione dati viene ad essere, ai fini qui in esame, la memorizzazione (temporanea o definitiva) degli stessi all'interno delle strutture di *cloud computing*. A ciò si aggiunga che tale profilo risulta poi accentuato poiché, proprio in ragione dell'ubiquità, il servizio offerto solitamente non si limita alla sola fornitura del *software*, ma comprende anche una funzione di *storage* correlata.

---

[36] Mediante i *service level agreement* vengono predefiniti i livelli di prestazione in ragione di parametri tecnici oggettivi e misurabili; cfr. A. Zincone, *Il contratto di outsourcing: natura, caratteristiche, effetti*, citato *supra*, 391 e 396 s., e F. Cardarelli, *La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing*, citato *supra*, 91 ss. Attualmente stanno tuttavia assumendo crescente rilievo, accanto agli SLA, i *Key Performance Indicators* (KPI), ovvero degli indici (qualitativi, quantitativi, di costo, di servizio), personalizzati in ragione delle specifiche di ciascuna azienda, mediante i quali è possibile monitorare l'andamento dei singoli processi aziendale, cfr. Politecnico di Milano-Dipartimento di Ingegneria Gestionale, *ICT Strategic Sourcing: nuovi equilibri oltre la crisi. Rapporto 2009 Osservatorio ICT Strategic Sourcing*, citato *supra*, 73.

[37] Cfr. a riguardo P. Hustinx (European Data Protection Supervisor), *Data protection and Cloud Computing under EU law*, relazione tenuta al Third European Cyber Security Awareness Day, BSA, European Parliament, 13 aprile 2010, in *www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf*, secondo cui « in many cases, one can probably argue that cloud providers are data processors. However, in practice, cloud computing services very often not only determine the means, but also to some extent the purposes of the processing, in which case they would be data controllers. Which role is played by cloud computing providers will need to be determined on a case by case basis ».

[38] L'elaborazione dati effettuata dal *software* in quanto tale è infatti attuata dall'utente legittimato all'uso del programma o, in taluni casi, è disposta direttamente dal produttore dell'applicativo (es. raccolta automatica di informazioni o invio/ricezione automatica dei dati).

In tal contesto, anche al di là della personalizzazione del servizio, le finalità e modalità di impiego del *software*, non in quanto tale (ciascun *software* è sotto quest'aspetto determinato dall'autore)[39], ma in relazione ai dati, appaiono definite dall'utente (SLA, possibilità di verifiche[40], ecc.), così come anche le scelte inerenti cosa salvare, modificare o rimuovere sui *data center*. Maggiore autonomia residua in materia di sicurezza in capo all'*outsourcee*, ma è altrettanto vero che le specifiche a riguardo vengono predefinite contrattualmente, ragion per cui risultano essere, almeno sotto i profili di maggior rilievo, delineate dall'*outsourcer* mediante clausole *ad hoc*[41].

Per tali ragioni si deve concludere che l'*outsourcer* riveste il ruolo di *controller* ed il fornitore del servizio quello di *processor*. Conferme in tal senso derivano inoltre dal fatto che l'attività di gestione demandata al fornitore del servizio riguarda solamente una parte dei trattamenti posti in essere dall'*outsourcer*[42] e che, come dimostrato dal processo stesso di esternalizzazione, il gestore del *cloud* SaaS non mostra una competenza professionale esclusiva così specifica e peculiare da svolgere un ruolo predominante in relazione alle dinamiche del trattamento e, conseguentemente, da comportare un elevato grado di autonomia, offrendo semmai uno *standard* tecnico-qualitativo superiore nell'erogazione di servizi precedentemente realizzati in azienda[43].

Il profilo attinente la memorizzazione dei dati, che si è visto determinante nella definizione del ruolo assunto dai soggetti nel mo-

---

[39] Sui profili inerenti i diritti di privativa sul *software* nel contesto dei processi di *outsourcing* informativo, cfr. A. Zincone, *Il contratto di outsourcing: natura, caratteristiche, effetti*, citato *supra*, 401 ss. e A. Musella, *Il contratto di* outsourcing *del sistema informativo*, citato *supra*, 877 ss.

[40] Con riguardo alla possibilità di verifiche, in relazione alla disciplina di cui all'art. 1662 c.c., cfr. A. Zincone, *Il contratto di outsourcing: natura, caratteristiche, effetti*, citato *supra*, 394 e M. Pittalis, *Outsourcing*, citato *supra*, 1019.

[41] Cfr. in proposito Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 14: « Determination of the 'means' therefore includes both technical and organizational questions where the decision can be well delegated to processors (as e.g. 'which hardware or software shall be used?') and essential elements which are traditionally and inherently reserved to the determination of the controller… while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means. In this perspective, it is well possible that the technical and organizational means are determined exclusively by the data processor ». Vero è che, in presenza di contratti *standard* con clausole non negoziabili o personalizzabili, sia i profili inerenti il servizio che quelli inerenti le misure di sicurezza vengono nei fatti predisposti unilateralmente dal fornitore, ma è pur anche vero che, recuperando la visione dato-centrica della direttiva, è l'*outsourcer* che, nello scegliere un dato servizio fra i diversi esistenti, viene a definire in maniera autonoma le modalità di gestione ed il regime di sicurezza cui assoggettare le informazioni.

[42] Cfr. Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 26.

[43] Cfr. Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 28.

dello SaaS rispetto al trattamento posto in essere, viene poi a costituire la natura stessa della prestazione nel caso di *cloud* IaaS (*infrastructure as a service*), consistente in via principale nel mettere a disposizione strutture *hardware* che offrono *storage* e connettività; ne consegue che la qualificazione giuridica del rapporto fra i soggetti nei termini sopra descritti (*controller-processor*) può essere a maggior ragione ribadita rispetto a tale servizio *cloud*. Né paiono mutare le valutazioni rispetto al più articolato *cloud* PaaS (*platform as a service*), laddove pare essere la pluralità degli applicativi, unitamente alla diversa finalità operativa degli stessi (agevolare lo sviluppo di un *software* e non fornire un programma già realizzato che soddisfi le esigenze dell'utente), a contraddistinguere l'offerta. Dal punto di vista del trattamento dati non ci si discosta dunque dal modello SaaS, essendo il trattamento comunque sostanzialmente finalizzato alla memorizzazione utile al funzionamento del *software* o alla conservazione del materiale mediante lo stesso realizzato[44].

Va da ultimo richiamato come, in virtù del disposto dell'art. 4, comma 1, della direttiva 95/46/CE, le regole comunitarie in materia di *data protection* siano destinate ad operare solamente quando il trattamento avvenga « in the context of the activities of an establishment of the controller on the territory of the Member State » oppure quando, in assenza di stabilimento, si faccia comunque ricorso a « equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community ». Ne consegue che, qualificando il fornitore di servizi di *cloud computing* quale *processor*, laddove l'*outsourcer* sia una società stabilita nell'UE non dovrebbero porsi problemi circa l'applicabilità delle disposizioni di derivazione comunitaria, salvi gli eventuali profili attinenti i flussi transfrontalieri di dati di cui al seguente paragrafo. Per altro, anche optando per una diversa qualificazione dell'*outsourcee* in termini di *controller* autonomo o contitolare, alla luce delle (pur opinabili) interpretazioni estensive suggerite a livello europeo e posto che i diversi servizi in questione comportano l'installazione sul terminale dell'utente di ben più di qualche *cookie*[45], po-

---

44 In termini generali, si può inoltre incidentalmente notare come il fornitore dei servizi di *cloud computing* rivesta invece la qualifica di *controller* rispetto ai dati di traffico inerenti la circolazione delle informazioni nel *cloud* (tra un *data center* ed un altro) o verso il *computer* dell'utente, in rapporto ai quali è titolare di un autonomo interesse imprenditoriale, così come, per analoga ragione, verrà ad assumere la stessa qualifica in relazione a tutti i dati attinenti il rapporto contrattuale.

45 Cfr. Articolo 29-Gruppo di lavoro per la tutela dei dati personali, *Tutela della vita privata su Internet - Un approccio integrato dell'EU alla protezione dei dati on-line* -, Bruxelles, 21 novembre 2000, 30 s., in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37it.pdf*, secondo cui rientrano nella nozione di « equipment » di cui all'art. 4, paragrafo 1, lett. *c*), dir. 95/46/CE, anche i *cookie*, per cui laddove essi vengano utilizzati per raccogliere dati destinati ad es-

trebbe giungersi alla medesima conclusione anche ove i *data center* fossero collocati al di fuori del perimetro comunitario ed il gestore degli stessi non fosse stabilito nell'UE.

3. (*Segue*): le implicazioni correlate alla connotazione transfrontaliera del trattamento.

Molti dei processi di *outsourcing* informatico, per ragioni sostanzialmente riconducibili al contenimento dei costi, attualmente si avvalgono di *outsourcee* collocati in nazioni diverse da quella in cui ha sede l'*outsourcer* e non di rado il flusso dati va dai Paesi più industrializzati verso quelli con inferiore progresso economico-sociale. Questo fenomeno, sotto il profilo giuridico, si traduce non solo nell'introduzione di elementi di internazionalità nel rapporto, ma spesso anche in un diverso livello di tutela assicurato ai diritti delle persone fisiche e giuridiche, nonché, talora, in un diverso margine di autonomia rispetto all'ingerenza dei poteri pubblici ed in un differente grado di democraticità di quest'ultimi. Tale profilo viene ora ad essere acuito nel caso di impiego di tecnologie di *cloud computing*, in virtù delle quali i dati possono essere distribuiti in vari *data center* ubicati in diverse nazioni. Può poi accadere — ad oggi più in relazione ai servizi di *cloud computing* pubblici o ibridi, piuttosto che a quelli privati[46] verso cui sembrano orientate le grandi aziende[47] — che il fornitore del

sere elaborati all'estero, « se il computer è ubicato in un paese dell'UE e il paese terzo si trova fuori dall'UE, quest'ultimo dovrà applicare alla raccolta di dati effettuata mediante il *cookie* i principi della legislazione nazionale di quello Stato membro ». Tale lettura « paneuropea » della lettera dell'art. 4 della direttiva 95/46/CE, ribadita nei successivi *Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca*, Bruxelles, 4 aprile 2008, 11, e *Parere 5/2009 sui social network on-line*, Bruxelles, 12 giugno 2009, 5, non pare tuttavia esente da critiche, cfr. in tal senso C. Kuner, *European data privacy law and online business*, Oxford-New York, 2003, 94 e 100 ss.

[46] Sotto il profilo dei modelli di sistema si suole infatti distinguere fra *private cloud* e *public cloud*, dove nel primo caso il servizio è erogato in favore di un solo soggetto, mentre nel secondo è rivolto al pubblico in genere (es. Amazon Web Services, Google AppEngine, Microsoft Windows Azure). Soluzioni intermedie sono poi il *community cloud* (destinato ad organizzazioni che intendono fruire in maniera condivisa del servizio) o l'*hybrid cloud*, che costituisce la commistione dei precedenti modelli e consente di potenziare le risorse del *private cloud* avvalendosi di quelle del *public cloud* laddove sia temporaneamente necessario. Ovviamente una struttura *cloud* privata può essere implementata e gestita direttamente dall'impresa che se ne avvale, ma tale ipotesi, mancando di elementi di *outsourcing*, non viene qui considerata. Per un maggior dettaglio circa le diverse tipologie cfr. Sun Microsystems, *Introduction to Cloud Computing Architecture. White Paper*, citato *supra*, 9 ss.

[47] Cfr. NextValue, *Cloud computing un anno dopo. CIO italiani e CIO europei a confronto*, citato *supra*, 28, fig. 9, ove, rispetto ad un campione di cento imprese con fatturato superiore a 100 milioni di euro, il 72% degli intervistati opta per un modello di *cloud* privata, il 13% per una ibrida ed il 5% per una pubblica. Tale quadro pare tuttavia destinato a mutare in favore delle soluzioni ibride tanto nei mercati esteri, più maturi per l'introduzione di tali tecnologie rispetto a quello italiano, quanto con riferimento alle realtà aziendali ita-

servizio abbia stipulato accordi contrattuali con altri soggetti per lo scambio di risorse informatiche, secondo un modello che ricorda quello degli accordi fra gestori dell'approvvigionamento di energia elettrica. Così quando un fornitore del servizio non ha sufficiente capacità (in termini ad esempio di *storage*) può utilizzare quella in eccesso di altri; da ciò deriva che i dati passano dall'*outsourcee* a terze parti, attraverso una serie di frammentazioni che può rendere arduo conoscere chi in un preciso istante sovrintenda allo loro gestione[48].

Può poi accadere, nel caso di SaaS, che il *software* offerto in modalità *cloud* da una società ICT all'azienda costituisca un'aggregazione di diversi servizi acquisiti dalla prima e cumulativamente offerti, ma individualmente erogati da separati fornitori sempre in modalità *cloud*, dando così vita ad una pluralità di relazioni negoziali ed al trasferimento dei dati fra più soggetti.

In termini generali va a riguardo osservato come la disciplina comunitaria abbia posto molta attenzione al profilo dei flussi transfrontalieri di dati, considerati, specie per le informazioni destinate a soggetti posti al di fuori del territorio comunitario, potenzialmente rischiosi per la tenuta dell'intero sistema di garanzie definite in materia[49]. Conseguentemente l'invio di informazioni personali verso un Paese terzo è ammessa solamente ove ai dati venga garantito « an adequate level of protection »[50], in maniera tale da non vanificare attraverso una simile operazione la protezione assicurata all'interno dell'Unione[51]. Laddove manchino tuttavia

liane di minori dimensioni. In particolare emerge in tali contesti una propensione ad avvalersi di *public cloud* per i servizi meno strategici (tra cui potrebbero rientrare la posta elettronica, l'organizzazione dell'agenda ecc.), ricorrendo invece a *private cloud* per la gestione dei dati meritevoli di maggiore tutela (es. dati finanziari o coperti da segreto industriale); cfr. per un'analisi di dettaglio con riferimento alle singole tipologie funzionali, IBM, *Diradare le nebbie attorno al cloud computing*, citato *supra*, 6 ss.

[48] Va in proposito aggiunto come, quando si fa riferimento ai dati aziendali gestiti attraverso *cloud computing*, debba tenersi anche conto delle copie di *back up* e delle copie replicate di tali dati, necessarie ai fini di sicurezza, rapidità e continuità di accesso. Ne consegue che di ogni dato vi sono più copie, potenzialmente collocabili in luoghi differenti fra loro.

[49] Se infatti all'interno dell'Unione, in virtù della dir. 95/46/CE — e delle successive direttive che l'hanno integrata su specifici temi —, si è venuta a creare una ben precisa sfera di protezione della persona con riferimento al trattamento dati, non altrettanto poteva dirsi al momento dell'approvazione della direttiva per la gran parte degli stati al di fuori dell'Unione, considerazione per altro ancor oggi valida per molte nazioni.

[50] Cfr. artt. 25 s., dir. 95/46/CE.

[51] Cfr. considerando n. 56, dir. 95/46/CE. Non va tuttavia trascurato il fatto che la direttiva comunitaria preveda diverse ipotesi di deroga in cui il trasferimento verso Paesi terzi può avvenire a prescindere dal rispetto del criterio dell'adeguatezza, ipotesi che hanno un certo rilievo in materia di *outsourcing*, concernendo il trasferimento di dati all'estero sulla base del consenso dell'interessato ovvero per il perseguimento di finalità contrattuali, cfr. art. 26, paragrafo 1, lett. *a*), *b*) e *c*), dir. 95/46/CE. In un'ottica di semplificazione degli adempimenti, di uniformità del trattamento e, soprattutto, di certezza delle situazioni giuridiche, pare tuttavia più agevole per l'impresa il ricorso alla diversa soluzione delle clausole-tipo, che esclude in radice tanto qualsiasi questione interpretativa circa la legittimità dell'applicazione del re-

congrue normative a tutela dei dati[52] è possibile fissare per contratto le garanzie minime a difesa dei soggetti interessati dal trattamento[53], anche avvalendosi delle clausole-tipo approvate dalla Commissione Europea[54].

Rispetto al contenuto delle clausole-tipo[55], che in molti casi rappresentano la soluzione più agevole[56], assume rilievo la clausola del terzo beneficiario[57] di cui si avvantaggia l'interessato dal trattamento che, in quanto estraneo all'accordo fra le parti che pongono in essere il flusso di dati, non potrebbe altrimenti far valere un proprio diritto *ex contractu* ad un trattamento conforme al contenuto delle clausole-tipo adottate, né nei confronti degli stipulanti, né (ove si verifichi il caso) degli ulteriori terzi cui vengano trasmessi i dati[58]. Ad ulteriore garanzia degli interessati ed in un'ottica volta a privilegiare l'ordinamento comunitario, nelle clausole approvate dalla Commissione si individua inoltre la legge

gime derogatorio, quanto la necessità di provvedere *ex ante* agli opportuni adempimenti, quale l'acquisizione del consenso *ad hoc*.

[52] Ad oggi è ancora limitato, in un'ottica mondiale, il numero di nazioni che hanno adottato soluzioni normative considerate dalla Commissione europea coerenti con i principi comunitari, cfr. *http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm*.

[53] Cfr. art. 26, paragrafi 2 e 4, dir. 95/46/CE. Ai sensi del paragrafo 1, lett. *a*), della norma citata sarebbe altresì possibile adottare la soluzione alternativa incentrata sul consenso dell'interessato al trasferimento dei dati, tuttavia tale soluzione, oltre a rendere opportuna un'adeguata previsione *ex ante* di tale eventualità, potrebbe comportare complicazioni nella gestione dei dati ove vi sia una successiva revoca del consenso prestato, cfr. in tal senso European Network and Information Security Agency (ENISA), *Cloud Computing. Benefits, risks and recommendations for information security*, novembre 2009, 103, in *www.enisa.europa.eu*.

[54] Cfr. Decisione della Commissione del 15 giugno 2001, C(2010)1539, poi modificata con Decisione della Commissione del 27 dicembre 2004 C(2004)5271, e Decisione della Commissione del 5 febbraio 2010, C(2010)593. In ragione della qualifica del rapporto fra *outsourcer* e fornitore del servizio *cloud* in termini rispettivamente di *controller* e *processor*, di cui *supra* nel testo, è tuttavia l'ultima delle tre decisioni richiamate a rilevare ai fini della presente analisi. Cfr. anche il 23º considerando della decisione del 5 febbraio 2010.

[55] Due le finalità principali di tali pattuizioni: la tutela dell'interessato e la responsabilizzazione dell' « esportatore » dei dati, ossia di colui che trasferisce i dati personali ad un terzo, detto « importatore », cfr. Decisione della Commissione del 5 febbraio 2010, C(2010)593, art. 3, lett. *c*) e *d*).

[56] Il ricorso alle clausole-tipo risulta preferibile rispetto alla redazione di pattuizioni sulle modalità di trattamento ad opera dalle parti, in ragione degli oneri procedurali previsti in quest'ultimo caso; laddove ci si discosti dai modelli predisposti a livello comunitario occorre infatti che la competente autorità nazionale autorizzi il trasferimento valutando l'adeguatezza della tutela offerta in via negoziale, cfr. art. 26 paragrafo 2, dir. 95/46/CE. Ne consegue il sorgere di un rischio correlato all'alea di tale giudizio e, dato non trascurabile in un'ottica d'impresa, l'incombere di oneri aggiuntivi sia in termini di adempimenti formali che di tempi procedurali.

[57] Cfr. Decisione della Commissione del 5 febbraio 2010, C(2010)593, Allegato, clausola n. 3; cfr. anche la successiva clausola n. 6 in materia di responsabilità.

[58] Cfr. Decisione della Commissione del 5 febbraio 2010, C(2010)593, Allegato, clausola n. 11, ove si prevede inoltre che occorra il preventivo consenso scritto dell'esportatore prima di stipulare tale subcontratto. La possibilità che vengano stipulati sub-contratti per l'esecuzione di un servizio di *cloud computing* dipende tanto dalla necessità di far ricorso a risorse informatiche di terze parti nel caso di saturazione delle proprie, quanto dal fatto che alcuni servizi forniti vengano in concreto erogati avvalendosi di soggetti diversi.

applicabile al contratto in quella del luogo di stabilimento dell'esportatore[59], che nel caso di servizi di *cloud computing* sarà l'impresa fruitrice degli stessi, con conseguente applicabilità del diritto comunitario per le imprese stabilite nell'Unione.

Più complessa appare invece l'ipotesi in cui il fornitore dei servizi di *cloud computing* (*processor*), stabilito nell'UE, si avvalga di terzi non ivi stabiliti per l'erogazione di parte dei servizi (*sub-processor*)[60], poiché in tal caso mancano clausole-tipo comunitarie *ad hoc*[61]. Tre le soluzioni possibili[62]: l'impiego delle clausole-tipo comunitarie direttamente ad opera del *controller* (i.e. il fruitore dei servizi di *cloud computing*) mediante un accordo con il *sub-processor*, che viene però in tal maniera considerato alla stregua di un *processor* importatore e non in quanto *sub-processor*; un mandato da parte del *controller* al *processor* affinché quest'ultimo stipuli in suo nome le clausole-tipo con il *sub-processor*; il ricorso a specifici accordi contrattuali fra le parti, previa autorizzazione dei competenti organi del Paese dell'esportatore.

Va infine osservato come in concreto, in un'ottica di semplificazione rispetto ai problemi inerenti il trattamento transfrontaliero dei dati, ma probabilmente anche per le diverse esigenze di garantire una maggior sicurezza della riservatezza delle informazioni rispetto ai poteri pubblici e di privilegiare contesti più sicuri e stabili, alcuni grandi fornitori di servizi di *cloud computing* hanno deciso di localizzare i propri *server cloud* nell'Unione europea[63]

---

[59] Cfr. Decisione della Commissione del 5 febbraio 2010, C(2010)593, Allegato, clausola n. 9.

[60] È l'ipotesi, di cui *supra* nel testo, nella quale il servizio in modalità *cloud* costituisce l'aggregazione dei diversi servizi cumulativamente offerti, ma individualmente erogati da separati fornitori, cui si aggiunge la diversa situazione in cui il gestore del *cloud* si avvalga di altre imprese cui delegare alcune funzioni operative, come ad es. la gestione dei *data center*.

[61] Cfr. Decisione della Commissione del 5 febbraio 2010, C(2010)593, Allegato, clausola n. 1, lett. *d*), che definisce *sub-processor* « any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract ». Si vedano a riguardo le considerazioni espresse in Articolo 29-Gruppo di lavoro per la tutela 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* (trasferimento da responsabile a incaricato del trattamento), Bruxelles, 5 marzo 2009, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp161_it.pdf*.

[62] Per un maggior dettaglio cfr. Article 29 Data Protection Working Party, *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, 4 ss., in *http://ec.europa.eu/justice_-home/fsj/privacy/docs/wpdocs/2010/wp176_en.pdf*.

[63] Va in proposito ricordato come nel caso di trattamento dati intracomunitario, stante la qualifica dell'*outsourcee* come *processor*, ai sensi dell'art. 17, paragrafo 3, dir. 95/46/CE le misure di sicurezza che devono essere da quest'ultimo adottate sono discipli-

(IBM) o, quantomeno, di lasciare al cliente la scelta fra più siti disponibili a livello mondiale (Microsoft), talora limitandone l'ubicazione solo agli USA o all'Unione europea (Google).

4. La sicurezza dei dati e delle informazioni aziendali.

Il profilo della sicurezza, per la natura dei dati elaborati, riveste da sempre un ruolo cruciale nella gestione delle informazioni archiviate nei *data base* aziendali; la centralità dell'*asset* informativo, anche in un'ottica competitiva, comporta infatti la necessaria adozione di soluzioni tecniche e procedimentali in grado di porre al riparo tanto le informazioni di carattere personale, quanto quelle coperte da segreto aziendale. Vari ed ormai noti alle prassi gestionali sono i rischi connessi, che, con particolare riferimento all'impiego degli strumenti informatici, possono essere raggruppati secondo la seguente quadripartizione basata sui fattori causali[64]: rischi ingenerati dal comportamento degli operatori[65], dal malfunzionamento dei sistemi[66], da azioni esterne[67], da eventi distruttivi. Ampio al riguardo il ventaglio delle soluzioni organizzative e tecniche maturare negli anni[68] volte al monitoraggio, al contenimento ed al contrasto di tali fattori avversi. Il quadro normativo, unitamente alle previsioni contrattuali diffuse nella prassi — specie per quanto concerne il segreto aziendale —[69], hanno poi affiancato alle regole tecniche specifiche regole comportamentali[70] definendo così un complesso sistema di tutela delle informazioni.

Rispetto a tale contesto l'avvento del *cloud computing*, mutando le modalità operative della fruizione delle risorse informatiche e, conseguentemente, informative, presenta in concreto non poche insidie sotto i menzionati profili[71], le quali, benché affrontabili

nate non dalla legge dello Stato del *controller*, ma « by the law of the Member State in which the processor is established ».

64 Sulla possibilità del ricorso allo strumento assicurativo per far fronte ai rischi informatici cfr. *supra* nota 6.

65 Si pensi, a titolo d'esempio, ai seguenti comportamenti: violazione delle procedure di autorizzazione ed autenticazione, violazione del segreto aziendale, negligenza o errori nella gestione delle informazioni.

66 Rientrano in tale ambito i potenziali pregiudizi causati da *deficit* di sicurezza dei sistemi rispetto all'azione di virus informatici o di programmi dannosi, da malfunzionamento degli strumenti, da vulnerabilità rispetto ad accessi esterni non autorizzati, da guasti ai sistemi complementari (impianti di alimentazione, di climatizzazione, ecc.).

67 Quali ad esempio accesso non autorizzato ai sistemi, intercettazione delle comunicazioni e attacchi informatici.

68 Soluzioni in parte anche indotte dall'attuazione delle misure di sicurezza previste dalla disciplina generale in materia di dati personali; cfr. art. 17, dir. 95/46/CE.

69 Cfr. A. Musella, *Il contratto di* outsourcing *del sistema informativo*, citato *supra*, 882 ss.

70 Sul rapporto fra norme tecniche e norme comportamentali in materia di trattamento dati sia consentito, in ragione dell'economia del presente contributo, rinviare a A. Mantelero, *Regole tecniche e regole giuridiche: interazioni e sinergie nella disciplina di Internet*, in *Contr. e impr.*, 2005, 678 ss.

71 L'adozione di tecniche di *cloud computing* basate sulla virtualizzazione

sul piano giuridico ricorrendo tanto a rimedi contrattuali quanto extracontrattuali, rappresentano una delle maggior criticità e causa di resistenza verso l'esternalizzazione dei servizi informatici[72]. Il passaggio al *cloud computing* comporta infatti per l'impresa, in maggior o minor maniera, la perdita del controllo materiale e diretto sulle risorse informatiche, deferendolo agli strumenti *software*[73] ed a quelli contrattuali (non a caso notevole rilievo è assunto dai *service level agreement*[74]), con un indebolimento sul piano dell'efficacia operativa.

In termini di sicurezza informatica le caratteristiche del servizio esaltano poi alcuni rischi già noti, *in primis* quello degli accessi illegittimi ai *data center* ad opera di « ladri di dati » o degli attacchi di tipo DDoS[75], laddove se da un lato una grande società di *cloud computing* effettua indubbiamente maggiori investimenti in tecnologie difensive rispetto ad una piccola o media impresa[76], è pur vero che la creazione di grandi aggregazioni di dati genera obiettivi ben visibili ed appetibili per gli autori degli illeciti.

Ai rischi « esterni » si cumulano inoltre quelli « interni », a partire, specie nei *cloud* SaaS e PaaS, dal vantaggio dell'aggiornamento in tempo reale dei *software* offerti che, sebbene elimini alcuni oneri[77], potrebbe rivelarsi potenzialmente dannoso laddove,

---

comporta poi l'affacciarsi di nuove problematiche in termini di sicurezza informatica con riguardo al flusso di dati che si genera fra macchine virtuali; cfr. B. SCHULTZ, *The Virtual Blind Spot*, 11 luglio 2010, in *www.cio.com*. In generale, circa i profili di sicurezza dei servizi *cloud computing*, si veda SUN MICROSYSTEMS, *Introduction to Cloud Computing Architecture. White Paper*, citato *supra*, 29 s., e per un'analisi dettagliata dei rischi cfr. EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA), *Cloud Computing. Benefits, risks and recommendations for information security*, citato *supra*. Sulla nozione di virtualizzazione, benché con riferimento ad alcuni specifici applicativi, cfr. *http://punto-informatico.it/2848215/PI/Approfondimenti/virtualizzazione-quali-vantaggi.aspx*.

[72] Cfr. NEXTVALUE, *Cloud computing un anno dopo. CIO italiani e CIO europei a confronto*, citato *supra*, 52, fig. 36 e cfr. POLITECNICO DI MILANO-DIPARTIMENTO DI INGEGNERIA GESTIONALE, *ICT Strategic Sourcing: nuovi equilibri oltre la crisi. Rapporto 2009 Osservatorio ICT Strategic Sourcing*, citato *supra*, 66 ss., laddove viene tuttavia riscontrato un disallineamento fra i timori per la sicurezza manifestati dalle imprese anteriormente all'adozione di una soluzione *cloud* e le valutazioni espresse *ex post*, tendenti a ridimensionare tale criticità.

[73] In termini di sicurezza dei dati questo si traduce anche in una maggior vulnerabilità del nuovo modello rispetto al precedente cui le informazioni potevano essere anche fisicamente separate in *hardware* differenti ed autonomamente messi in sicurezza.

[74] La rilevanza del profilo contrattuale inerente i livelli di prestazioni è poi acuita dalla pluralità di soggetti coinvolti per il buon funzionamento dell'« ecosistema » *cloud*, non solo il gestore del servizio di *cloud computing*, ma anche i fornitori di accesso alle reti telematiche ed i gestori delle stesse, da ciascuno dei quali occorrerà ricevere precise rassicurazioni in via contrattuale circa i parametri qualitativi di servizio garantiti.

[75] Si tratta di attacchi informatici, solitamente realizzati a scopo estorsivo, mediante i quali vengono saturate le risorse di un sistema informatico, rendendolo instabile, ricorrendo all'invio sistematico di una grande massa di richieste.

[76] In tal senso il ricorso al *cloud computing* può comportare per tali imprese un innalzamento dei livelli di sicurezza in termini di gestione dei rischi, *business continuity* e *disaster recovery*.

[77] In specie viene meno il gravoso problema delle migrazioni dei vari elaboratori da una vecchia versione del programma operativo o del sistema ad una più recente.

come già accaduto, i nuovi programmi presentino difetti o vulnerabilità di rilievo, o comunque una peggior funzionalità. Sempre in ragione del struttura del servizio, va altresì osservato come la polverizzazione dei dati distribuiti all'interno del *cloud* comporti l'ulteriore problema della certezza circa l'effettiva eliminazione delle informazioni ove questa venga predisposta dal fruitore del servizio[78].

Benché tali criticità non sembrino in grado di arrestare la progressiva migrazione verso il *cloud computing*, in ragione delle stesse potrebbe risultare utile affiancare alle tutele già offerte dall'informatica[79], dalle norme e dai contratti, efficaci soluzioni assicurative per far fronte ai danni potenziali che, in caso di perdita o furto di informazioni, potrebbero raggiungere anche notevoli entità in ragione della quantità e della natura dei dati interessati.

Passando invece dal livello « micro », inerente le qualità ed i dettagli del servizio offerto, a quello « macro », concernente la struttura del mercato e delle offerte in materia di *cloud computing*, sono poi ravvisabili ulteriori e diverse criticità[80] destinate ad incidere sull'appetibilità della nuova soluzione tecnologica. Nello specifico potrebbero emergere effetti negativi qualora si realizzassero processi di concentrazione, indotti anche dall'entità delle risorse necessarie per competere nel mercato del *cloud computing*, tali da limitare a poche grandi multinazionali l'offerta dei servizi *cloud* destinati alle imprese, dando luogo non solo ad un accentramento dei *data center*, ma anche all'accumulo nelle mani di un ristretto numero di soggetti privati di un'immensa mole di informazioni.

In proposito una prima eventualità sfavorevole potrebbe essere rappresentata dalle conseguenze di potenziali difetti di funzionamento: con i dati nel *cloud* ed i *server* ospitanti non raggiungibili, migliaia di imprese cesserebbero di operare. L'« oligarchia dei fornitori » potrebbe poi indurre eventuali abusi in termini di violazione della riservatezza delle informazioni acquisite[81] (secondo

[78] Nello specifico una rimozione completa delle informazioni può risultare materialmente difficile sia per la creazione di varie copie di servizio (finalizzate al *back up*, al *mirorring*, al *disaster recovery*, ecc.), sia, nel caso di *public cloud*, per la coesistenza sui supporti fisici di memorizzazione di dati appartenenti a clienti diversi, con conseguenti limiti ad un'eliminazione definitiva senza la compromissione delle informazioni di terze parti.

[79] Cfr. IBM, *Cloud Security Guidance. IBM Recommendations for the Implementation of Cloud Security*, 2009, 7 ss., in *www.redbooks.ibm.com/redpapers/pdfs/redp4614.pdf*.

[80] Una disamina delle differenti criticità, informatiche e non, legate all'adozione di servizi erogati in modalità *cloud* si legge in AA.VV., *Above the Clouds: A Berkeley View of Cloud Computing*, citato *supra*, 14 ss.

[81] Limitatamente al profilo inerente il trattamento dei dati personali, va in proposito tenuto presente che, qualificato l'*outsourcee* come *processor*, laddove quest'ultimo elabori i dati in maniera infedele per fini propri, verrebbe a mutare la sua veste giuridica, assumendo il ruolo di *controller*

un copione per altro ad oggi non ignoto alle cronache, anche italiane, in materia di ICT), rispetto ai quali sarebbero forse da adottare soluzioni incentrate quantomeno sull'obbligo di notifica per la creazione dei *data center* aventi maggior rilevanza, in ragione delle dimensioni o della natura dei dati, e sulla vigilanza ad opera di organi pubblici *ad hoc* sulla gestione di tali archivi, secondo un modello che ricorda in parte le prime leggi sulla protezione dei dati (non a caso nate in un'epoca dominata dai *main frame*).

I processi di concentrazione potrebbero altresì ingenerare aumenti dei costi dei servizi, barriere alla migrazione da un fornitore all'altro[82] o alla fruizione di servizi *cloud* erogati da soggetti diversi[83], con conseguenze in termini di libertà della gestione dei dati, posto che, sposato in maniera netta un modello *cloud*, potrebbe essere difficile tanto ritornare ad una gestione interna, quanto sottrarsi agli eventuali limiti posti all'interoperabilità dei sistemi, se non a prezzo di costi significativi.

È dunque forse per l'insieme di tutti questi motivi che ad oggi, sebbene cresca l'interesse verso le nuove tecnologie *cloud*, le

(cfr. in tal senso ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 1/2010 on the concepts of « controller » and « processor »*, citata *supra*, 14), da cui consegue, al di là delle implicazioni in termini di responsabilità fra le parti e verso i terzi, che il trattamento posto in essere risulterà necessariamente illegittimo, mancando l'informativa e (ove necessario) il consenso degli interessati. Con riguardo alle informazioni coperte da segreto aziendale è poi possibile introdurre nei contratti di *cloud computing* clausole volte a costituire obblighi di riservatezza assistite da penali. Rispetto ad entrambe le tipologie di dati si può inoltre far ricorso a soluzioni di tipo tecnico-informatico in grado di limitare gli accessi illegittimi, sia perché attuati da soggetti non autorizzati, sia perché animati da finalità illecite. Nello specifico l'impiego della crittografia, per i dati in transito oggetto di trasferimento da/verso i *data center*, come per quelli ivi residenti, nonché il ricorso a sistemi di autenticazione informatica « robusti » per aver certezza dell'identità dei soggetti legittimati all'accesso ai dati ed alla ricezione degli stessi (tanto all'interno del gestore *cloud*, quanto nel rapporto fra *outsourcer* ed *outsourcee*), potrebbero concorrere nella riduzione dei rischi.

[82] Cfr. *Open Cloud Manifesto*, 2009, 6, in *www.opencloudmanifesto.org*, in cui si afferma: « Cloud providers must not use their market position to lock customers into their particular platforms and limit their choice of providers »; cfr. inoltre, con riguardo all'*outsourcing* informatico in generale, P. VARÌ, Outsourcing *di servizi informatici*, in *Inf. e dir.*, 1995, 95.

[83] Centrale a riguardo il profilo dell'interoperabilità dei sistemi; cfr. *Open Cloud Manifesto*, citato *supra*, 4, in cui si afferma che « Cloud providers need to support interoperability standards so that organizations can combine any cloud provider's capabilities into their solutions ». All'*Open Cloud Manifesto* hanno aderito oltre 300 società e gruppi, tra cui alcuni dei principali operatori del settore ICT mondiale (IBM, Cisco, AMD, AT&T, ecc.), cfr. http://www.opencloudmanifesto.org/supporters.htm. In proposito cfr. anche EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA), *Cloud Computing. Benefits, risks and recommendations for information security*, citato *supra*, 25 ss., secondo cui « there is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data and service portability… This makes it extremely difficult for a customer to migrate from one provider to another, or to migrate data and services to or from an in-house IT environment e si ravvisa in tale limite un rischio elevato collegato all'adozione di sistemi *cloud*, in ragione dei costi di migrazione e dei danni potenziali in caso di fallimento del fornitore del servizio. Si vedano inoltre AA.VV., *Above the Clouds: A Berkeley View of Cloud Computing*, citato *supra*, 15 e INTERNATIONAL TELECOMMUNICATION UNION, *Distributed Computing: Utilities, Grid & Clouds*, citato *supra*, 7 ss.

aziende si mostrano ancora restie ad adottarle o quantomeno ad impiegarle per i servizi a maggiore criticità[84], benché a riguardo potrebbe assistersi ad un'evoluzione differenziata in ragione della distribuzione asimmetrica della consapevolezza dei rischi: mentre le grandi imprese, più consapevoli e con maggiori dotazioni, potrebbero guardare a soluzioni mirate di *private cloud*, le medie e soprattutto le piccole, allettate dalla possibilità di avere a costi contenuti servizi di categoria superiore e meno consce dei rischi (anche per carenza di competenze interne), potrebbero invece optare per un ampio ricorso al *cloud*, anche « pubblico »[85], con sottostima delle criticità cui espongono sé stesse ed i propri clienti[86].

Per l'insieme dei motivi ora evidenziati, ancorché la diffusione del *cloud computing* sia solo agli inizi[87] e dunque, come ogni altra tecnologia e modello organizzativo, necessiti di un tempo sufficiente per sviluppare le opportune risposte alle criticità, non pare tuttavia possibile delegare soltanto al mercato ed ai tecnologi il compito di superare i limiti attuali. L'uno e gli altri potranno infatti validamente adoperarsi in tal senso[88], ma il conseguimento di

[84] Cfr. IBM, *Cloud computing White paper. IBM Point of View: Security and Cloud Computing*, novembre 2009, 7, in *www.ibm.com/common/ssi/fcgi-bin/ssialias?infotype=SA&subtype=WH&appname=SWGE_TI_SE_USEN&htmlfid=TIW14045USEN&attachment=TIW14045USEN_HR.PDF*.

[85] Cfr. *supra* nota 46.

[86] Cfr. B. Schultz, *The Virtual Blind Spot*, citato *supra*, in cui viene riportato il parere di un analista di Forrester, secondo cui « Many companies that have virtualized environments haven't contemplated the security ramifications of what they're doing yet ».

[87] In questa fase iniziale non sono mancate vittime illustri dei disguidi tecnico-informatici, così Google ha dovuto riconoscere la presenza di un *bug* nel programma Google Docs, un sistema SaaS di videoscrittura e scambio documenti, da cui è derivato, ancorché per un numero minimo di soggetti, la comunicazione involontaria di alcuni dei propri documenti presenti nella *cloud* a terzi e ad insaputa degli interessati; cfr. *On Yesterday's email*, 7 marzo 2009, in *http://googledocs.blogspot.com/2009/03/on-yesterdays-email.html* e *Google Discloses Privacy Glitch*, in *The Wall Street Journal*, 8 marzo 2009, in *http://blogs.wsj.com/digits/2009/03/08/1214*.

[88] Con riguardo ai profili tecnologici e di procedimentalizzazione delle modalità di gestione assumono, in particolare, rilievo le iniziative di standardizzazione attualmente in corso cfr. in specie gli standard ISO/IEC CD 29100 (Information technology-Security techniques-Privacy framework) e ISO/IEC CD 29101 (Information technology-Security techniques-Privacy reference architecture) in corso di definizione. Si vedano altresì i già esistenti ISO/IEC 27001:2005 (Information technology-Security techniques-Information security management systems-Requirements) ed ISO/IEC 27002:2005 (Information technology-Security techniques-Code of practice for information security management), nonché, con riferimento ai processi di *outsourcing* in genere, lo Statement on Auditing Standard (SAS-70). In merito al processo di standardizzazione, si vedano però anche le osservazioni critiche espresse nell'*Open Cloud Manifesto*, citato *supra*, 6, ove si afferma: « IT industry has invested heavily in existing standards and standards organizations; there is no need to duplicate or reinvent them. 4. When new standards (or adjustments to existing standards) are needed, we must be judicious and pragmatic to avoid creating too many standards. We must ensure that standards promote innovation and do not inhibit it ». La standardizzazione va inoltre considerata sotto il profilo della trasparenza e semplificazione nell'individuazione del livello di protezione offerto dal fornitore del servizio, mediante il rinvio ad una valutazione unitaria sulla conformità a determinate specifiche. In tal maniera si riducono potenzialmente gli oneri di redazione contrattuale rispetto alla definizione dei profili tecnici e si sgravano gli utenti dalla disami-

un adeguato livello di tutela dei diversi interessi in gioco potrà essere raggiunto solo mediante un efficace intervento anche sul piano giuridico[89], non sottovalutando l'opportunità di istituti di controllo e, soprattutto, dando vita a forme di collaborazione efficienti e rapide a livello globale, stanti le dimensioni del fenomeno e dei principali attori coinvolti.

na dei singoli contratti ed accordi sui livelli di servizio per avere conoscenza delle principali modalità di trattamento delle informazioni.

[89] Pare in proposito opportuno, proprio in ragione della natura dei servizi, ipotizzare soluzioni efficaci di monitoraggio dell'agire del gestore del *cloud computing*, incentrate su soluzioni quali il ricorso a verifiche ad opera di terze parti, il rilascio di rapporti periodici sul servizio, la tracciabilità informatica delle azioni poste in essere dal fornitore del servizio. In tal senso, limitatamente ai dati personali, sembrano andare le recenti indicazioni di cui all'Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, Bruxelles, 13 luglio 2010, in *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp173_en.pdf*, laddove, ritenendo che « responsibility and accountability are two sides of the same coin and both essential elements of good governance. Only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed », si auspica, nell'ottica della revisione della direttiva 95/46/CE, l'introduzione di una nuova disposizione che obblighi il *controller* ad adottare « appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with » ed a dimostrare « compliance » rispetto a tale obbligo « to the supervisory authority on its request ».