01037/12/IT
WP 196

Parere 05/2012 sul *cloud computing*

adottato il 1° luglio 2012

Il gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e cittadinanza) della Commissione europea, direzione generale Giustizia, B-1049 Bruxelles, Belgio, ufficio MO-59 02/013.
Sito Internet: http://ec.europa.eu/justice/data-protection/index_it.htm

[NdT] Ai fini del presente parere, con "responsabile del trattamento" e con "incaricato del trattamento" si intendono rispettivamente il "titolare" e il "responsabile" di cui all'articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

Sintesi

Nel presente parere il Gruppo di lavoro articolo 29 prende in esame tutte le questioni rilevanti per i fornitori di servizi di *cloud computing* operanti nello Spazio economico europeo (SEE) e per i loro clienti, specificando tutti i principi applicabili della direttiva UE sulla protezione dei dati (95/46/CE) e della direttiva e-privacy 2002/58/CE (modificata dalla direttiva 2009/136/CE), dove pertinenti.

Malgrado i vantaggi riconosciuti del *cloud computing* in termini economici e sociali, il presente parere sottolinea come la diffusione su vasta scala dei servizi di *cloud computing* comporti una serie di rischi per la protezione dei dati, in particolare una mancanza di controllo sui dati personali, nonché informazioni insufficienti in merito alle modalità, al luogo e all'esecutore del trattamento/subtrattamento dei dati. Gli enti pubblici e le imprese private che intendono avvalersi di servizi di *cloud computing* devono valutare attentamente questi rischi. Il presente parere esamina i problemi connessi con la condivisione di risorse con altre parti, la scarsa trasparenza di una catena di esternalizzazione costituita da molteplici incaricati del trattamento e subcontraenti, la mancanza di un quadro di riferimento comune globale sulla portabilità dei dati e l'incertezza in merito all'ammissibilità del trasferimento di dati personali a fornitori di servizi *cloud* al di fuori del SEE. Allo stesso modo, nel parere viene messa in evidenza come fonte di grave preoccupazione la mancanza di trasparenza in termini di informazioni che un responsabile del trattamento è in grado di fornire a un interessato sulle modalità di trattamento dei suoi dati personali. Gli interessati devono[1] essere informati su chi procede al trattamento dei loro dati e per quali finalità e per essere in grado di esercitare i diritti loro spettanti a tale proposito.

Una conclusione fondamentale del presente parere è il fatto che imprese e amministrazioni che intendono utilizzare servizi di *cloud computing* dovrebbero innanzitutto effettuare un'analisi del rischio completa e approfondita. Tutti i fornitori di servizi *cloud* nel SEE dovrebbero fornire al cliente tutte le informazioni necessarie per valutare correttamente i pro e i contro dell'adozione di un simile servizio. Sicurezza, trasparenza e certezza giuridica per i clienti dovrebbero essere principi fondamentali alla base dell'offerta di servizi di *cloud computing*.

Nelle raccomandazioni contenute nel presente parere si mettono in evidenza le responsabilità del cliente di servizi *cloud* in quanto responsabile del trattamento e si raccomanda pertanto che il cliente selezioni un fornitore che garantisca la conformità alla normativa UE in materia di protezione dei dati. Riguardo alla necessità di adeguate garanzie contrattuali, il parere prevede che un contratto tra cliente e fornitore di servizi *cloud* debba fornire garanzie sufficienti in termini di misure tecniche e organizzative. È importante anche la raccomandazione secondo cui il cliente dovrebbe verificare se il fornitore può garantire la legalità di eventuali trasferimenti transfrontalieri di dati.

[1] In questo caso, "devono" traduce il termine inglese "must". Si ritiene opportuno specificare che i termini chiave "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", e "OPTIONAL" nel presente documento si devono interpretare come descritto nella RFC 2119. Il documento è disponibile all'indirizzo http://www.ietf.org/rfc/rfc2119.txt. Tuttavia, ai fini di una maggiore leggibilità, i termini non sono scritti in lettere maiuscole.

Come in qualsiasi processo evolutivo, la diffusione del *cloud computing* come paradigma tecnologico globale rappresenta una sfida. Il presente parere, in quanto tale, si può considerare un passo importante nel definire i compiti che la comunità della protezione dei dati dovrà assumere a questo proposito nei prossimi anni.

Indice

1. Introduzione

Per alcuni, il *cloud computing* è una delle maggiori rivoluzioni tecnologiche emerse in tempi recenti. Per altri, è solo la naturale evoluzione di una serie di tecnologie mirate a realizzare il sogno atteso da tempo dell'*utility computing*. In ogni caso, numerosi soggetti portatori di interesse hanno messo in primo piano il *cloud computing* nella definizione delle loro strategie tecnologiche.

Il *cloud computing* consiste in una serie di tecnologie e modelli di servizio incentrati sull'uso e sulla fornitura di applicazioni informatiche, capacità di elaborazione e archiviazione e spazio di memoria basati su Internet. Il *cloud computing* può produrre importanti vantaggi economici, poiché su Internet è possibile configurare, espandere e accedere a risorse su richiesta con molta facilità. Oltre ai vantaggi economici, il *cloud computing* può anche offrire vantaggi in termini di sicurezza; le imprese, in particolare piccole e medie, possono acquistare ad un costo marginale tecnologie avanzate che altrimenti non sarebbero alla loro portata.

I servizi offerti dai fornitori di soluzioni di *cloud computing* sono molto diversificati e spaziano da sistemi elaborativi virtuali (che sostituiscono o si affiancano ai tradizionali *server* controllati direttamente dal responsabile del trattamento dei dati) a servizi di supporto allo sviluppo e per l'*hosting* evoluto delle applicazioni, sino a soluzioni *software* rese disponibili in modalità *web* che sono sostitutive delle tradizionali applicazioni installate sui computer degli utenti finali, quali ad esempio applicazioni per l'elaborazione dei testi, per la gestione di agende e calendari, cartelle per l'archiviazione dei documenti *on-line* e soluzioni esternalizzate di posta elettronica. Alcune delle definizioni più comunemente utilizzate per questi diversi tipi di servizi sono contenute nell'Allegato al presente parere.

Nel suo parere, il Gruppo di lavoro articolo 29 (in appresso WP 29) prende in esame il diritto applicabile e gli obblighi dei responsabili del trattamento di dati nello Spazio economico europeo (in appresso SEE) e dei fornitori di servizi *cloud* con clienti nel SEE. La situazione analizzata dal parere ipotizza una relazione tra responsabile e incaricato del trattamento dei dati, dove il cliente è il responsabile e il fornitore di servizi *cloud* è l'incaricato. Nei casi in cui il fornitore di servizi funge anche da responsabile del trattamento dei dati occorre rispettare ulteriori requisiti. Di conseguenza, una condizione essenziale per avvalersi di servizi di *cloud computing* è che il responsabile del trattamento dei dati effettui un'adeguata valutazione del rischio, che comprenda l'ubicazione dei *server* dove si elaborano i dati e l'analisi di rischi e benefici nell'ottica della protezione dei dati, secondo i criteri esposti nelle sezioni che seguono.

Il presente parere specifica i principi applicabili a responsabili e incaricati del trattamento dei dati ai sensi della direttiva generale sulla protezione dei dati (95/46/CE), quali specificazione e limitazione della finalità, cancellazione dei dati e misure tecniche e organizzative. Il parere fornisce indicazioni sui requisiti in fatto di sicurezza, in termini di garanzie strutturali e procedurali. Inoltre, pone un particolare accento sulle disposizioni contrattuali che dovrebbero regolamentare la relazione tra responsabile e incaricato del trattamento. I classici obiettivi di sicurezza dei dati sono disponibilità, integrità e riservatezza. Tuttavia, poiché la protezione dei dati non si limita alla sicurezza, questi obiettivi sono integrati dai principi di trasparenza, isolamento, possibilità di intervento e portabilità specifici della protezione dei dati, a conferma del diritto dell'individuo alla protezione dei dati di cui all'articolo 8 della Carta dei diritti fondamentali dell'UE.

Per quanto concerne il trasferimento di dati personali fuori dal SEE, si prendono in esame strumenti quali clausole contrattuali tipo adottate dalla Commissione europea, accertamenti di adeguatezza e possibili future norme vincolanti d'impresa (BCR) per gli incaricati del trattamento, nonché i rischi per la protezione dei dati derivanti da richieste di autorità internazionali di contrasto del crimine.

Il parere si conclude con una serie di raccomandazioni per i clienti *cloud* in quanto responsabili del trattamento, per i fornitori *cloud* in quanto incaricati del trattamento e per la Commissione europea in merito a futuri cambiamenti nel quadro europeo in materia di protezione dei dati.

Nell'aprile 2012 il Gruppo di lavoro internazionale di Berlino sulla protezione dei dati nelle telecomunicazioni ha adottato il *Memorandum di Sopot*[2] che esamina gli aspetti della privacy e della protezione dei dati nel *cloud computing* e sottolinea che questo nuovo sistema non deve comportare un abbassamento degli standard di protezione dei dati rispetto alle procedure tradizionali di trattamento dei dati.

2. Rischi del *cloud computing* per la protezione dei dati

Poiché il presente parere si concentra sulle operazioni di trattamento di dati personali che si avvalgono di servizi di *cloud computing* sono presi in considerazione solo i rischi specifici relativi a tale contesto[3]. La maggioranza di questi rischi rientra in due ampie categorie, e precisamente la mancanza di controllo sui dati e la carenza di informazioni concernenti il trattamento stesso (assenza di trasparenza). I rischi specifici del *cloud computing* considerati nel presente parere comprendono quanto segue.

Mancanza di controllo

Affidando dati personali a sistemi gestiti da un fornitore di servizi *cloud*, i clienti rischiano di perdere il controllo esclusivo dei dati e di non poter prendere le misure tecniche e organizzative necessarie per garantire la disponibilità, l'integrità, la riservatezza, la trasparenza, l'isolamento[4], la portabilità dei dati e la possibilità di intervento sugli stessi. Questa mancanza di controllo si può manifestare nel seguente modo:

- Mancanza di disponibilità dovuta alla scarsa interoperabilità (*vendor lock-in,* dipendenza nei confronti di un unico fornitore): se il fornitore *cloud* si basa su una tecnologia esclusiva, per un cliente *cloud* può rivelarsi difficile trasferire dati e documenti tra diversi sistemi *cloud* (portabilità dei dati) o scambiare informazioni con entità che utilizzano servizi *cloud* gestiti da fornitori diversi (interoperabilità).
- Mancanza di integrità dovuta alla condivisione di risorse: un sistema *cloud* è costituito da sistemi e infrastrutture condivisi; i fornitori *cloud* trattano dati personali derivanti da un'ampia gamma di fonti, in termini di interessati e organizzazioni, ed è possibile che sorgano conflitti d'interesse e/o divergenza di obiettivi.

---

2 http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

3 Oltre ai rischi relativi ai dati personali oggetto di trattamento "nel *cloud*" citati esplicitamente nel presente parere, occorre tenere conto anche di tutti i rischi relativi all'esternalizzazione del trattamento di dati personali.

4 In Germania è stato introdotto il concetto più ampio di "unlinkability", o impossibilità di collegamento. Cfr. nota 24 sotto.

- Mancanza di riservatezza in termini di richieste di autorità di contrasto dirette a un fornitore *cloud*: i dati personali trattati nel sistema *cloud* possono essere oggetto di richieste di informazioni a fini di contrasto della criminalità da parte delle competenti autorità degli Stati membri dell'UE e di paesi terzi. Esiste il rischio che si possano divulgare dati personali ad agenzie di contrasto (straniere) senza una valida base giuridica UE, configurando pertanto una violazione della legislazione UE sulla protezione dei dati.
- Scarsa possibilità di intervento dovuta alla complessità e alle dinamiche della catena di esternalizzazione (*outsourcing*): il servizio *cloud* offerto da un fornitore potrebbe derivare dalla combinazione di servizi di una serie di altri fornitori, che si possono aggiungere o eliminare dinamicamente nel corso della durata del contratto del cliente.
- Scarsa possibilità di intervento (diritti degli interessati): è possibile che un fornitore *cloud* non preveda le misure e gli strumenti necessari per assistere il responsabile del trattamento nella gestione dei dati, ad esempio in termini di accesso, cancellazione o correzione dei dati.
- Mancanza di isolamento: un fornitore *cloud* può servirsi del controllo fisico di dati di clienti diversi per mettere in collegamento dati personali. Se agevolati da diritti di accesso sufficientemente privilegiati (ruoli ad alto rischio), gli amministratori possono collegare informazioni provenienti da diversi clienti.

Mancanza di informazioni sul trattamento (trasparenza)

La disponibilità di informazioni insufficienti sulle operazioni di trattamento nei servizi *cloud* rappresenta un rischio per i responsabili del trattamento e per gli interessati, che potrebbero non essere consapevoli di potenziali rischi e minacce e pertanto non prendere misure appropriate.

Alcune potenziali minacce possono derivare dal fatto che il responsabile del trattamento non sappia che

- si sta verificando un trattamento a catena che coinvolge molteplici incaricati e subcontraenti;
- i dati personali sono trattati in diverse località geografiche all'interno del SEE, con dirette conseguenze sul diritto applicabile in eventuali controversie sulla protezione dei dati che possano sorgere tra utente e fornitore del servizio;
- i dati personali sono trasferiti a paesi terzi al di fuori del SEE. Questi paesi potrebbero non offrire un livello adeguato di protezione dei dati e i trasferimenti potrebbero non essere salvaguardati da misure adeguate (ad esempio clausole contrattuali tipo o norme vincolanti d'impresa) e risultare, pertanto, illegali.

È essenziale che gli interessati i cui dati personali sono oggetto di trattamento in un sistema *cloud* siano informati in merito all'identità del responsabile del trattamento e alla finalità dello stesso (un requisito previsto per tutti i responsabili del trattamento ai sensi della direttiva sulla protezione dei dati 95/46/CE). Considerando la potenziale complessità delle catene di trattamento in un ambiente di *cloud computing*, al fine di garantire un trattamento leale nei confronti dell'interessato (articolo 10 della direttiva 95/46/CE), i responsabili dovrebbero, anche a titolo di buona prassi, fornire ulteriori informazioni relativamente ai (sub-)incaricati che forniscono servizi *cloud*.

3. Quadro giuridico

3.1 Quadro in materia di protezione dei dati

Il quadro giuridico pertinente è la direttiva sulla protezione dei dati 95/46/CE, che si applica a tutti i casi di trattamento di dati personali nell'ambito di servizi di *cloud computing*. La direttiva e-privacy 2002/58/CE (modificata dalla direttiva 2009/136/CE) si applica al trattamento di dati personali in relazione alla fornitura di servizi di comunicazione elettronica disponibili al pubblico nelle reti pubbliche di comunicazione (operatori delle telecomunicazioni) e pertanto è pertinente se tali servizi sono forniti mediante una soluzione *cloud*[5].

3.2 Diritto applicabile

I criteri per stabilire l'applicabilità della legislazione sono contenuti nell'articolo 4 della direttiva 95/46/CE, che si riferisce al diritto applicabile ai responsabili del trattamento[6] con una o più sedi all'interno del SEE e anche al diritto applicabile ai responsabili del trattamento stabiliti al di fuori del SEE, ma che utilizzano attrezzature situate all'interno del SEE per il trattamento dei dati personali. Il Gruppo di lavoro articolo 29 ha analizzato la questione nel suo parere 8/2010 sul diritto applicabile[7].

Nel primo caso, il fattore che determina l'applicazione della normativa UE al responsabile del trattamento è l'ubicazione della sua sede e delle attività svolte, secondo l'articolo 4, paragrafo 1, lettera a) della direttiva, mentre la tipologia del modello di servizio *cloud* è irrilevante. La legislazione applicabile è la legge del paese dov'è stabilito il responsabile del trattamento che appalta servizi di *cloud computing* piuttosto che il luogo dove sono situati i fornitori di tali servizi.

Se il responsabile del trattamento ha sede in vari Stati membri e il trattamento di dati rientra nelle attività svolte in tali paesi, il diritto applicabile sarà quello di ciascuno degli Stati membri in cui viene effettuato il trattamento.

L'articolo 4, paragrafo 1, lettera c)[8] si riferisce alle modalità di applicazione della legislazione sulla protezione dei dati ai responsabili del trattamento che non sono stabiliti nel SEE ma ricorrono a strumenti automatizzati o non automatizzati situati nel territorio dello Stato membro, a meno che questi non siano utilizzati ai soli fini di transito. Ciò significa che se un cliente *cloud* è stabilito al di fuori del SEE ma incarica un fornitore *cloud* con sede nel SEE, il fornitore esporta la legislazione sulla protezione dei dati al cliente.

---

5 Direttiva 2002/58/CE sulla e-privacy (modificata dalla direttiva 2009/136/CE): la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche si applica ai fornitori di servizi di comunicazione elettronica accessibili al pubblico e impone loro di garantire il rispetto degli obblighi relativi alla segretezza della comunicazione e alla protezione dei dati personali, nonché i diritti e gli obblighi concernenti le reti e i servizi di comunicazione elettronica. Quando forniscono servizi di comunicazione elettronica disponibili al pubblico, i fornitori di servizi di *cloud computing* sono soggetti a questa direttiva.

6 Il concetto di responsabile del trattamento si trova nell'articolo 2, lettera h) della direttiva ed è stato analizzato dal Gruppo di lavoro articolo 29 nel suo parere 1/2010 sui concetti di responsabile del trattamento e incaricato del trattamento.

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_it.pdf

8 L'articolo 4, paragrafo 1, lettera c) stabilisce che la legislazione di uno Stato è applicabile quando il responsabile del trattamento "non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea".

3.3 Compiti e responsabilità di diversi attori

Come già accennato, il *cloud computing* coinvolge una serie di diversi operatori ed è importante valutare e chiarire il ruolo di ciascuno di essi al fine di stabilire i rispettivi obblighi specifici per quanto concerne l'attuale legislazione in materia di protezione dei dati.

Va ricordato che il Gruppo di lavoro articolo 29, nel suo parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento", rileva che "*il concetto di responsabile del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati, e il modo in cui gli interessati possono esercitare in pratica i loro diritti - serve, in altre parole, ad attribuire responsabilità*". Questi due criteri generali di responsabilità dell'osservanza e di attribuzione della responsabilità dovrebbero essere tenuti presenti dalle parti interessate nel corso dell'analisi in questione.

3.3.1 Cliente *cloud* e fornitore *cloud*

Il cliente *cloud* determina la finalità ultima del trattamento e decide in merito all'esternalizzazione di tale trattamento e alla delega ad un'organizzazione esterna delle attività di trattamento, in tutto o in parte. Il cliente *cloud* agisce pertanto in qualità di responsabile del trattamento dei dati. La direttiva definisce il responsabile del trattamento come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento dei dati personali*". Il cliente *cloud* in quanto responsabile del trattamento deve accettare la responsabilità dell'osservanza della legislazione sulla protezione dei dati ed è soggetto a tutti gli obblighi di legge di cui alla direttiva 95/46/CE. Il cliente *cloud* può incaricare il fornitore *cloud* della scelta dei metodi e delle misure tecniche e organizzative da utilizzare per conseguire gli scopi del responsabile del trattamento.

Il fornitore *cloud* è l'entità che fornisce i servizi di *cloud computing* nelle varie forme discusse sopra. Quando fornisce gli strumenti e la piattaforma, agendo per conto del cliente *cloud*, il fornitore *cloud* è considerato alla stregua di un incaricato del trattamento, ossia, secondo la direttiva 95/46/CE "*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento"* [9][10].

Come affermato nel parere 1/2010, per valutare la responsabilità del trattamento si possono utilizzare alcuni criteri[11]. In effetti, si possono presentare situazioni in cui un fornitore di servizi *cloud* può essere considerato corresponsabile o responsabile a pieno titolo, a seconda delle circostanze concrete. Ad esempio, potrebbe trattarsi del caso in cui il fornitore procede al trattamento di dati per scopi propri.

Va sottolineato che, anche in contesti complessi di trattamento di dati personali in cui intervengono vari responsabili, è essenziale garantire l'osservanza delle norme sulla protezione dei dati e una chiara attribuzione delle responsabilità per possibili violazioni di tali norme. Questo per evitare che venga meno la protezione dei dati personali, che si generi un

---

9 Il parere riguarda solo la regolare relazione responsabile del trattamento – incaricato del trattamento.

10 L'ambiente del *cloud computing* può essere utilizzato anche da persone fisiche (utenti) per svolgere esclusivamente attività personali o nazionali. In tal caso, occorre valutare attentamente se si applica la cosiddetta "esenzione domestica" che esenta gli utenti dalla qualifica di responsabile del trattamento. Tuttavia, la questione non rientra nell'ambito di applicazione del presente parere.

11 Ad es. livello di istruzioni, controllo da parte del cliente *cloud*, competenza delle parti.

"conflitto di competenze negativo" o si producano delle falle, in una situazione in cui nessuna delle parti si assumerebbe gli obblighi o assicurerebbe i diritti derivanti dalla direttiva.

Nell'attuale scenario del *cloud computing*, i clienti di servizi di *cloud computing* potrebbero non avere margine di manovra nel negoziare i termini contrattuali dell'uso dei servizi *cloud*, che in molti casi sono caratterizzati da offerte standardizzate. In ogni caso, alla fine è il cliente che decide in merito all'assegnazione di parte o della totalità del trattamento a servizi *cloud* per scopi specifici; il punto fondamentale in questo caso è che il ruolo del fornitore *cloud* sarà quello di un contraente nei confronti del cliente. Come affermato nel parere 1/2010[12] sui concetti di "responsabile del trattamento" e "incaricato del trattamento" del Gruppo di lavoro articolo 29 "*lo squilibrio fra il potere contrattuale di un piccolo responsabile del trattamento rispetto a un grosso fornitore di servizi non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati*". Per questo motivo, il responsabile del trattamento deve scegliere un fornitore *cloud* che garantisca l'osservanza della normativa in materia di protezione dei dati. Un'enfasi particolare va posta sulle caratteristiche dei contratti applicabili, che devono prevedere una serie di garanzie standard per la protezione dei dati, ivi comprese quelle descritte dal Gruppo di lavoro nelle sezioni 3.4.3 (Misure tecniche e organizzative) e 3.5 (Trasferimenti internazionali), nonché su meccanismi aggiuntivi che si possono dimostrare adeguati per agevolare la *due diligence* e la responsabilità (quali *audit* di terzi indipendenti e certificazioni dei servizi di un fornitore – cfr. sezione 4.2).

I fornitori di servizi di *cloud computing* (in quanto incaricati del trattamento) hanno il dovere di garantire la riservatezza. La direttiva 95/46/CE stabilisce che: "*L'incaricato del trattamento o chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento, non deve elaborare i dati personali ai quali ha accesso, se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi legali*". Anche l'accesso ai dati da parte del fornitore *cloud* durante la prestazione del servizio è fondamentalmente disciplinato dall'obbligo di rispettare le disposizioni dell'articolo 17 della direttiva (cfr. sezione 3.4.2.).

Gli incaricati del trattamento devono tenere conto del tipo di soluzione *cloud* in questione (pubblica, privata, di comunità o ibrida / IaaS, SaaS or PaaS [cfr. Allegato a) Modelli di *rollout* - b) Modelli di erogazione dei servizi]) e del tipo di servizio acquistato dal cliente. Gli incaricati del trattamento sono responsabili dell'adozione di misure di sicurezza in linea con quanto previsto dalla normativa UE applicata nelle giurisdizioni del responsabile del trattamento e dell'incaricato del trattamento. Inoltre, gli incaricati del trattamento sono tenuti ad assistere il responsabile del trattamento nel rispettare i diritti (esercitati) degli interessati.

3.3.2 Subcontraenti

I servizi di *cloud computing* possono comportare il coinvolgimento di una serie di parti contraenti che fungono da incaricati dal trattamento. Inoltre, è comune che gli incaricati del trattamento designino dei subincaricati che quindi ottengono l'accesso ai dati personali. Se appaltano dei servizi a subcontraenti, gli incaricati del trattamento sono obbligati a informarne il cliente, descrivendo nel dettaglio il tipo di servizio concesso in subappalto, le caratteristiche dei subcontraenti attuali o potenziali e le garanzie offerte da queste entità al fornitore di servizi di *cloud computing* ai fini dell'osservanza della direttiva 95/46/CE.

[12] Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento" - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_it.pdf

Tutti gli obblighi pertinenti si applicano pertanto anche ai subcontraenti, tramite contratti stipulati tra il fornitore *cloud* e il subcontraente che rispecchino le disposizioni del contratto tra cliente e fornitore *cloud*. Nel suo parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento", il Gruppo di lavoro articolo 29 fa riferimento alla molteplicità di incaricati del trattamento nei casi in cui questi ultimi possono avere una relazione diretta con il responsabile o operare in qualità di subcontraenti ai quali gli incaricati del trattamento delegano parte delle attività di trattamento loro affidate. "*Nulla, nella direttiva, impedisce che, per motivi organizzativi, più entità possano essere designate come incaricati o subcontraenti, anche suddividendo i compiti rilevanti. Nel procedere all'elaborazione dei dati tutti questi soggetti, però, devono attenersi alle istruzioni date dal responsabile del trattamento*"[13].

In simili scenari, gli obblighi e le responsabilità derivanti dalla legislazione sulla protezione dei dati devono essere chiaramente attribuiti e non si devono disperdere lungo la catena di esternalizzazione o di subappalto, al fine di garantire un effettivo controllo e l'attribuzione di chiare responsabilità per le attività di trattamento.

Un possibile modello di garanzie che si possono utilizzare per chiarire i compiti e gli obblighi degli incaricati del trattamento quando concedono in subappalto l'attività di trattamento è stato introdotto per la prima volta dalla decisione della Commissione del 5 febbraio 2010 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi[14]. In questo modello il subtrattamento è consentito solo previo consenso scritto del responsabile del trattamento e previo accordo scritto che imponga al subincaricato gli stessi obblighi dell'incaricato del trattamento. Se il subincaricato non adempie agli obblighi di protezione dei dati a norma di tale accordo scritto, l'incaricato del trattamento risponde a pieno titolo nei confronti del responsabile del trattamento per l'esecuzione degli obblighi del subincaricato ai sensi di tale accordo. Una disposizione di questo tipo potrebbe essere inserita in qualsiasi clausola contrattuale tra un responsabile del trattamento e un fornitore *cloud* che intenda affidare servizi a subcontraenti, per assicurare le garanzie richieste per il subtrattamento.

Una soluzione analoga concernente le garanzie nel corso del subtrattamento è stata proposta recentemente dalla Commissione nella proposta di un regolamento generale sulla protezione dei dati[15]. Le azioni di un incaricato del trattamento devono essere disciplinate da un contratto o altro atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente, tra l'altro, che l'incaricato del trattamento ricorra ad un altro incaricato del trattamento solo previa autorizzazione del responsabile del trattamento (articolo 26, paragrafo 2, della proposta).

Secondo il parere del WP29, l'incaricato del trattamento può subappaltare le sue attività esclusivamente previo consenso del responsabile del trattamento, che di norma può essere concesso all'inizio del servizio[16] con un chiaro obbligo per l'incaricato di informare il responsabile del trattamento di eventuali cambiamenti concernenti l'aggiunta o la sostituzione di subincaricati, mentre il responsabile del trattamento si riserva la possibilità in qualsiasi momento di opporsi a tali cambiamenti o di risolvere il contratto. Dovrebbe sussistere un

---

13 Cfr. WP169, pag. 29, parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento" (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_it.pdf)

14 Cfr. FAQ II.5 WP176.

15 Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, 25.1.2012.

16 Cfr. FAQ II, 1) WP176, adottato il 12 luglio 2010.

chiaro obbligo a carico del fornitore di servizi *cloud* di indicare tutti i subcontraenti incaricati. Inoltre, il fornitore *cloud* e il subcontraente sono tenuti a stipulare un contratto che rispecchi le clausole del contratto stipulato tra cliente e fornitore *cloud*. Il responsabile del trattamento dovrebbe essere in grado di avvalersi di possibilità di ricorso in caso di violazioni dei contratti da parte di subincaricati. Si potrebbe provvedere in tal senso garantendo che l'incaricato del trattamento risponda direttamente nei confronti del responsabile del trattamento in caso di violazioni provocate da un subincaricato, o creando un diritto del terzo a vantaggio del responsabile del trattamento nei contratti conclusi tra incaricato del trattamento e subincaricati, ovvero in virtù del fatto che tali contratti saranno firmati per conto del responsabile del trattamento dei dati, che quindi diventa parte contraente.

3.4 Obblighi di protezione dei dati nella relazione cliente-fornitore

3.4.1 Osservanza dei principi fondamentali

La legittimità del trattamento di dati personali in servizi di *cloud computing* dipende dall'osservanza di principi fondamentali della legislazione UE in materia di protezione dei dati: in particolare, dev'essere garantita la trasparenza nei confronti degli interessati, dev'essere rispettato il principio della specificazione e limitazione delle finalità e i dati personali devono essere cancellati non appena la loro conservazione non è più necessaria. Inoltre, devono essere attuate opportune misure tecniche e organizzative per garantire un livello adeguato di protezione e sicurezza dei dati.

3.4.1.1 Trasparenza

La trasparenza è fondamentale per il trattamento equo e legittimo dei dati personali. La direttiva 95/46/CE obbliga il cliente *cloud* a fornire all'interessato, presso il quale raccoglie dati che lo riguardano, informazioni sulla sua identità e sulla finalità del trattamento. Il cliente *cloud* è inoltre tenuto a fornire ulteriori informazioni, ad esempio relative ai destinatari o alle categorie di destinatari dei dati, che possono anche comprendere incaricati e subincaricati del trattamento nella misura in cui tali ulteriori informazioni siano necessarie per garantire un trattamento leale nei confronti dell'interessato (cfr. articolo 10 della direttiva)[17].

La trasparenza dev'essere garantita anche nel rapporto tra cliente *cloud*, fornitore *cloud* e (eventuali) subcontraenti. Il cliente *cloud* è in grado di valutare la legittimità del trattamento di dati personali nei servizi *cloud* solo se il fornitore del servizio lo informa in merito a tutte le questioni pertinenti. Un responsabile del trattamento che preveda di ingaggiare un fornitore *cloud* dovrebbe verificare attentamente i termini e le condizioni di tale fornitore e valutarli dal punto di vista della protezione dei dati.

Ai fini della trasparenza nel *cloud computing* occorre che il cliente *cloud* sia a conoscenza di tutti i subcontraenti che contribuiscono all'erogazione del servizio *cloud*, nonché dell'ubicazione di tutti i centri presso i quali può essere effettuato il trattamento dei dati personali[18].

Se l'erogazione di un servizio richiede l'installazione di software sui sistemi del cliente *cloud* (ad es. *browser plug-in*), il fornitore *cloud* è tenuto, a titolo di buona prassi, ad informare il cliente di questa circostanza e in particolare delle sue implicazioni dal punto di vista della

---

[17] Un obbligo corrispondente di informare l'interessato sussiste quando dati che non sono stati ottenuti dallo stesso interessato, bensì da fonti diverse, vengano registrati o divulgati a un terzo (cfr. articolo 11).

[18] Solo in tal caso sarà in grado di valutare se i dati personali possono essere trasferiti a un cosiddetto paese terzo al di fuori dello Spazio economico europeo (SEE) che non garantisce un adeguato livello di protezione ai sensi della direttiva 95/46/CE. Cfr. anche la sezione 3.4.6 in appresso.

protezione e della sicurezza dei dati. Viceversa, il cliente *cloud* dovrebbe sollevare la questione *ex ante*, se non è affrontata in misura sufficiente dal fornitore *cloud*.

3.4.1.2 Specificazione e limitazione della finalità

Il principio della specificazione e limitazione della finalità richiede che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità (cfr. articolo 6, paragrafo 1, lettera b) della direttiva 95/46/CE). Il cliente *cloud* deve determinare la finalità del trattamento prima di procedere alla raccolta di dati personali dall'interessato, informandolo in proposito. Il cliente *cloud* non deve trattare dati personali per finalità diverse che non siano compatibili con quelle originali.

Inoltre, occorre garantire che i dati personali non siano (illegalmente) trattati per ulteriori finalità dal fornitore del servizio *cloud* o da uno dei suoi subcontraenti. Poiché un tipico scenario di servizi *cloud* può facilmente coinvolgere un maggior numero di subcontraenti, il rischio del trattamento di dati personali per ulteriori finalità incompatibili dev'essere considerato particolarmente alto. Per ridurre al minimo tale rischio, il contratto tra fornitore e cliente *cloud* dovrebbe prevedere misure tecniche e organizzative intese a mitigarlo e fornire garanzie in merito alla registrazione (*logging*) e all'*audit* di operazioni di trattamento di dati personali eseguite da dipendenti del fornitore *cloud* o subcontraenti[19]. Il contratto dovrebbe prevedere sanzioni contro il fornitore o il subcontraente in caso di violazione della legislazione sulla protezione dei dati.

3.4.1.3 Cancellazione dei dati

A norma dell'articolo 6, paragrafo 1, lettera e), della direttiva 95/46/CE, i dati personali devono essere conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. I dati personali che non sono più necessari devono essere cancellati o resi anonimi. Ove non sia possibile cancellarli a causa di norme di legge sulla conservazione (ad es. normative fiscali), l'accesso a tali dati personali dev'essere bloccato. Spetta al cliente *cloud* garantire che i dati personali siano cancellati non appena non siano più necessari nel senso sopra indicato[20].

Il principio della cancellazione dei dati si applica ai dati personali a prescindere dal fatto che siano memorizzati su disco rigido o altri supporti per la conservazione dei dati (ad es. nastri per *backup*). Poiché i dati personali possono essere conservati in sovrabbondanza su diversi *server* in diversi luoghi, occorre garantire che in ciascun caso siano cancellati in modo irrecuperabile (vale a dire che devono essere cancellati anche versioni precedenti, *file* temporanei e persino frammenti di *file*).

I clienti *cloud* devono essere consapevoli del fatto che i dati di *log*[21] che agevolano la verifica, la conservazione, la modifica o la cancellazione dei dati possono anch'essi essere qualificati come dati personali relativi all'interessato che ha avviato la relativa operazione di trattamento[22].

La cancellazione sicura dei dati personali impone che i supporti di memorizzazione vengano distrutti o smagnetizzati o che i dati personali conservati siano effettivamente cancellati

---

19 Cfr. sezione 3.4.3 in appresso.

20 La cancellazione dei dati è una questione pertinente per tutta la durata di un contratto di *cloud computing* e alla sua conclusione. È pertinente anche in caso di sostituzione o ritiro di un subcontraente.

21 Osservazioni sui requisiti di *logging* seguono al punto 4.3.4.2.

22 Questo significa che occorre definire i periodi ragionevoli di conservazione per *file* di *log* e stabilire le procedure per garantire la cancellazione puntuale o l'anonimizzazione di tali dati.

mediante sovrascrittura. Per la sovrascrittura di dati personali si dovrebbero utilizzare speciali strumenti *software* che sovrascrivono più volte i dati, conformemente a specifiche riconosciute.

Il cliente *cloud* dovrebbe assicurarsi che il fornitore *cloud* garantisca la cancellazione sicura nel senso sopra citato e che il contratto tra il fornitore e il cliente contenga chiare disposizioni per la cancellazione dei dati personali[23]. Lo stesso vale per i contratti tra fornitori *cloud* e subcontraenti.

3.4.2 Garanzie contrattuali della relazione "responsabile del trattamento"-"incaricato del trattamento"

Quando decidono di affidarsi a servizi di *cloud computing*, i responsabili del trattamento sono tenuti a scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e all'organizzazione dei trattamenti da effettuare e devono assicurarsi del rispetto di tali misure (articolo 17, paragrafo 2, direttiva 95/46/CE). Inoltre, sono legalmente obbligati a firmare un contratto formale con il fornitore di servizi *cloud*, come previsto dall'articolo 17, paragrafo 3, della direttiva 95/46/CE, che stabilisce che la relazione tra responsabile e incaricato del trattamento sia disciplinata da un contratto o un altro atto giuridico vincolante. Ai fini di conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativi alla protezione dei dati e i requisiti relativi alle misure tecniche e organizzative sono stipulati per iscritto o in altra forma equivalente.

Il contratto deve almeno stabilire, in particolare, che l'incaricato del trattamento è tenuto a seguire le istruzioni del responsabile del trattamento e a mettere in atto le misure tecniche e organizzative necessarie per proteggere adeguatamente i dati personali.

Al fine di garantire la certezza giuridica, il contratto deve prevedere anche i seguenti aspetti:

1. dettagli sulle istruzioni del cliente (misura e modalità) da trasmettere al fornitore del servizio, con particolare riguardo per gli accordi sul livello del servizio (SLA) applicabili (che dovrebbero essere oggettivi e misurabili) e le sanzioni pertinenti (finanziarie o altro, ivi compresa la possibilità di citare in giudizio il fornitore in caso di inadempienza).
2. Specificazione delle misure di sicurezza che il fornitore *cloud* è tenuto a rispettare, a seconda dei rischi del trattamento e della natura dei dati da proteggere. È molto importante che siano specificate misure tecniche e organizzative concrete, come quelle delineate nella sezione 3.4.3 che segue, ferma restando l'applicazione di eventuali misure più rigorose previste dalla legislazione nazionale del cliente.
3. Oggetto e orizzonte temporale del servizio *cloud* da fornire, nonché portata, modalità e finalità del trattamento di dati personali effettuato dal fornitore *cloud* e tipologia dei dati personali oggetto del trattamento.
4. Specificazione delle condizioni per la restituzione dei dati (personali) o per la loro distruzione una volta concluso il servizio. Inoltre, occorre garantire la cancellazione sicura dei dati personali su richiesta del cliente *cloud*.
5. Inserimento di una clausola di riservatezza vincolante per il fornitore *cloud* e per eventuali suoi dipendenti che abbiano accesso ai dati. Possono accedere ai dati esclusivamente persone autorizzate.

[23] Cfr. sezione 3.4.3 in appresso.

6. Obbligo a carico del fornitore di sostenere il cliente nell'agevolare l'esercizio dei diritti degli interessati di accedere ai loro dati, nonché rettificarli o cancellarli.
7. Il contratto dovrebbe stabilire espressamente che il fornitore *cloud* non può comunicare i dati a terzi, anche per motivi di conservazione, a meno che nel contratto sia prevista la presenza di subcontraenti. Il contratto dovrebbe specificare che i subincaricati possono essere autorizzati solo sulla base di un consenso che di norma può essere concesso dal responsabile del trattamento a fronte di un chiaro obbligo dell'incaricato del trattamento di informarlo in merito a eventuali cambiamenti previsti in proposito, mentre il responsabile del trattamento si riserva la possibilità, in qualsiasi momento, di opporsi a tali cambiamenti o di risolvere il contratto. Il contratto dovrebbe chiarire l'obbligo del fornitore *cloud* di indicare tutti i subcontraenti autorizzati (ad es. in un registro digitale pubblico). Occorre garantire che i contratti stipulati tra fornitore *cloud* e subcontraenti rispecchino le disposizioni del contratto stipulato tra cliente e fornitore *cloud* (ossia che i subincaricati siano soggetti agli stessi obblighi contrattuali del fornitore *cloud*). In particolare, occorre garantire che il fornitore *cloud* e tutti i subcontraenti agiscano esclusivamente secondo le istruzioni del cliente *cloud*. Come spiegato nel capitolo sul subtrattamento, il contratto dovrebbe definire chiaramente la catena della responsabilità e prevedere l'obbligo dell'incaricato del trattamento di strutturare i trasferimenti internazionali, ad esempio firmando contratti con subincaricati sulla base delle clausole contrattuali tipo contenute nella decisione 2010/87/UE.
8. Chiarimento della responsabilità del fornitore *cloud* di comunicare al cliente *cloud* eventuali violazioni che influiscano sui suoi dati.
9. Obbligo del fornitore *cloud* di fornire un elenco dei luoghi dove può avere luogo il trattamento dei dati.
10. Diritto del responsabile del trattamento di controllare e corrispondente obbligo del fornitore *cloud* di cooperare.
11. Il contratto dovrebbe stabilire che il fornitore *cloud* è tenuto a informare il cliente in merito a cambiamenti rilevanti concernenti il servizio *cloud*, come l'attuazione di funzioni aggiuntive.
12. Il contratto dovrebbe prevedere attività di *logging* e *auditing* delle operazioni di trattamento di dati personali svolte dal fornitore *cloud* o da subcontraenti.
13. Notifica del cliente *cloud* in merito a eventuali richieste legalmente vincolanti di divulgare dati personali presentate da un'autorità di contrasto, salvo che tale divulgazione sia comunque vietata, ad esempio ai sensi del diritto penale per preservare la riservatezza di un'indagine giudiziaria.
14. Obbligo generale a carico del fornitore del servizio di assicurare che la sua organizzazione interna e i suoi sistemi di trattamento dei dati (e quelli di eventuali subincaricati) sono conformi agli obblighi e alle norme di legge vigenti, nazionali e internazionali.

In caso di violazione da parte del responsabile del trattamento, chiunque subisca un danno a causa di un trattamento illegale ha il diritto di ricevere un risarcimento dal responsabile del trattamento per il danno causato. Qualora utilizzino i dati per qualsiasi altra finalità, ovvero li comunichino o li utilizzino in un modo che costituisce violazione del contratto, anche gli incaricati del trattamento sono considerati alla stregua del responsabile del trattamento e s'intendono responsabili delle violazioni nelle quali sono coinvolti personalmente.

Va notato che, in molti casi, i fornitori di servizi di *cloud computing* offrono servizi e contratti standard da far firmare ai responsabili del trattamento, fissando di fatto una certa modalità-tipo di trattamento dei dati personali. Questo squilibrio fra il potere contrattuale di un piccolo responsabile del trattamento rispetto a un grosso fornitore di servizi non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati.

3.4.3 Misure tecniche e organizzative per la protezione e la sicurezza dei dati

L'articolo 17, paragrafo 2, della direttiva 95/46/CE conferisce ai clienti *cloud* (in qualità di responsabili del trattamento) la piena responsabilità della scelta di fornitori *cloud* che adottino misure di sicurezza tecniche e organizzative adeguate per proteggere i dati personali e siano in grado di dimostrare senso di responsabilità.

In aggiunta agli obiettivi di sicurezza fondamentali, quali disponibilità, riservatezza e integrità, occorre prestare attenzione anche agli obiettivi complementari in fatto di protezione dei dati quali trasparenza (cfr. 3.4.1.1 sopra), isolamento [24], possibilità di intervento, responsabilità e portabilità. La presente sezione mette in evidenza questi obiettivi centrali per la protezione dei dati, fatte salve altre analisi del rischio complementari, orientate alla sicurezza[25].

3.4.3.1 Disponibilità

Garantire la disponibilità significa assicurare un accesso tempestivo e affidabile ai dati personali.

Una grave minaccia alla disponibilità nel *cloud computing* è la perdita accidentale di connettività di rete tra il cliente e il fornitore o il malfunzionamento del *server* provocato da atti dolosi quali attacchi DoS (Denial of Service) distribuiti[26]. Altri rischi per la disponibilità comprendono guasti accidentali dell'*hardware* sulla rete e nei sistemi *cloud* di trattamento e conservazione dei dati, interruzioni di corrente e altri problemi infrastrutturali.

I responsabili del trattamento dei dati dovrebbero controllare se il fornitore *cloud* ha adottato misure ragionevoli per far fronte al rischio di interruzioni, quali *link* di *backup* in Internet, dispositivi di archiviazione ridondante e meccanismi efficaci di *backup* dei dati.

3.4.3.2 Integrità

L'integrità si può definire come la proprietà per cui i dati sono autentici e non sono stati alterati intenzionalmente o accidentalmente durante il trattamento, l'archiviazione o la trasmissione. Il concetto di integrità si può estendere ai sistemi informatici e richiede che il trattamento dei dati personali in tali sistemi resti inalterato.

Le alterazioni ai dati personali si possono individuare con meccanismi di autenticazione crittografica, quali codici di autenticazione di messaggi o firme.

Le interferenze nell'integrità dei sistemi informatici nel *cloud computing* si possono impedire o individuare mediante sistemi per l'identificazione / prevenzione di intrusioni (IPS / IDS). Si

---

[24] In Germania, nella legislazione è stato introdotto il concetto più ampio di "unlinkability", o impossibilità di collegamento, promosso dalla Conferenza dei commissari per la protezione di dati.

[25] Cfr. ad es. ENISA all'indirizzo http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[26] Un attacco DoS è un tentativo coordinato di rendere un computer o una risorsa di rete inaccessibile ai suoi utenti autorizzati, in via temporanea o definitiva (ad esempio mediante numerosi sistemi di attacco che paralizzano l'obiettivo con una moltitudine di richieste esterne di comunicazione).

tratta di un aspetto particolarmente importante nel genere di ambienti di reti aperte dove operano di norma i servizi *cloud*.

3.4.3.3 Riservatezza

In un ambiente *cloud*, il criptaggio può contribuire in misura significativa alla riservatezza dei dati personali, se attuato correttamente, benché non li renda anonimi in modo irreversibile[27]. Si dovrebbe ricorrere al criptaggio dei dati personali in tutti i casi di dati "in transito" e quando disponibile per dati "a riposo"[28]. In alcuni casi (ad es., un servizio di archiviazione IaaS) un cliente *cloud* può scegliere di non affidarsi a una soluzione di criptaggio offerta dal fornitore *cloud*, ma di criptare i dati personali prima di inviarli al sistema *cloud*. Il criptaggio dei dati a riposo richiede una particolare attenzione per la gestione della chiave crittografica, poiché la sicurezza dei dati in ultima analisi dipende dalla riservatezza delle chiavi di criptaggio.

Le comunicazioni tra fornitore e cliente di servizi *cloud* e tra centri di trattamento dati dovrebbero essere criptate. La gestione a distanza della piattaforma *cloud* dovrebbe avvenire esclusivamente tramite un canale di comunicazione sicuro. Se un cliente prevede non solo di archiviare, ma anche di procedere all'ulteriore trattamento dei dati nel sistema *cloud* (ad es., consultando schede in banche dati) deve tenere presente che il criptaggio non può essere mantenuto durante il trattamento dei dati (tranne per calcoli molto specifici).

Ulteriori misure tecniche intese a garantire la riservatezza comprendono i meccanismi di autorizzazione e autenticazione (ad es. l'autenticazione a due fattori). Le clausole contrattuali dovrebbero anche imporre obblighi di riservatezza ai dipendenti di clienti *cloud*, fornitori *cloud* e subcontraenti.

3.4.3.4 Trasparenza

Le misure tecniche e organizzative devono promuovere la trasparenza per consentire le verifiche (cfr. 3.4.1.1.).

3.4.3.5 Isolamento (limitazione della finalità)

Nelle infrastrutture *cloud*, risorse quali dispositivi di archiviazione, memorie e reti sono condivise da molti utenti, con la conseguenza di nuovi rischi di divulgazione e trattamento dei dati per scopi illegittimi. L'obiettivo di protezione "isolamento" è inteso ad affrontare questo aspetto e a contribuire a garantire che i dati non vengano utilizzati al di là delle finalità iniziali (articolo 6, paragrafo 1, lettera b), della direttiva 95/46/CE) e a mantenere la riservatezza e l'integrità[29].

L'isolamento richiede innanzi tutto una *governance* adeguata dei diritti e dei ruoli per l'accesso ai dati personali, verificata su base periodica. Si dovrebbe evitare l'attribuzione di ruoli con privilegi eccessivi (ad esempio, nessun utente o amministratore dovrebbe essere autorizzato ad accedere all'intero sistema *cloud*). Più in generale, amministratori e utenti devono poter accedere esclusivamente alle informazioni necessarie per le loro finalità legittime (principio del privilegio minimo).

---

[27] Direttiva 95/46/CE – considerando 26: "(...); che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile; (...)". I processi di frammentazione dei dati tecnici che si possono utilizzare nel quadro della fornitura di servizi di *cloud computing* non portano all'anonimato irreversibile e pertanto non implicano la mancata applicazione degli obblighi di tutela dei dati.

[28] Questo è vero in particolare per i responsabili del trattamento che intendono trasferire al sistema *cloud* dati sensibili ai sensi dell'articolo 8 della direttiva 95/46/CE (quali dati sanitari) o che sono soggetti a specifici obblighi legali di segretezza professionale.

[29] Cfr. 3.4.1.2.

In secondo luogo, l'isolamento dipende anche da misure tecniche quali l'*hardening* di ipervisori e la gestione corretta di risorse condivise, se si utilizzano macchine virtuali per condividere risorse fisiche tra diversi client *cloud*.

3.4.3.5 Possibilità di intervento

La direttiva 95/46/CE conferisce alle persone interessate i diritti di accesso, rettifica, cancellazione, blocco e opposizione (cfr. articoli 12 e 14). Il cliente *cloud* deve verificare che il fornitore *cloud* non ponga ostacoli tecnici e organizzativi a questi requisiti, anche nei casi di ulteriore trattamento dei dati da parte di subcontraenti.

Il contratto tra cliente e fornitore dovrebbe stabilire che il fornitore *cloud* ha l'obbligo di sostenere il cliente nell'agevolare l'esercizio dei diritti degli interessati e di garantire che lo stesso valga nelle relazioni con eventuali subcontraenti[30].

3.4.3.6 Portabilità

Attualmente, la maggior parte dei fornitori di servizi *cloud* non utilizzano formati di dati standard e interfacce che facilitano l'interoperabilità e la portabilità tra diversi fornitori. Se un cliente *cloud* decide di migrare da un fornitore ad un altro, questa mancanza di interoperabilità può rendere impossibile, o comunque molto difficoltoso, trasferire i dati (personali) del cliente al nuovo fornitore *cloud* (il cosiddetto *vendor lock-in*). Lo stesso vale per i servizi sviluppati dal cliente su una piattaforma offerta dal fornitore originario (PaaS). Prima di ordinare un servizio *cloud*, il cliente *cloud* dovrebbe controllare se e come il fornitore garantisce la portabilità di dati e servizi[31].

3.4.3.7 Responsabilità

Nelle tecnologie informatiche, si può definire la responsabilità come la capacità di stabilire che cosa ha fatto un'entità in un determinato momento nel passato e come lo ha fatto. Nel campo della protezione dei dati spesso assume un significato più ampio e descrive la capacità delle parti di dimostrare di aver preso misure adeguate per garantire l'attuazione dei principi di tutela dei dati.

La responsabilità nelle tecnologie informatiche assume una particolare importanza per indagare su violazioni dei dati personali, dove clienti *cloud*, fornitori e subcontraenti possono avere ciascuno un certo grado di responsabilità operativa. La capacità della piattaforma *cloud* di fornire meccanismi di monitoraggio e *logging* affidabili e completi riveste un'importanza fondamentale a questo proposito.

Inoltre, i fornitori di servizi *cloud* dovrebbero fornire prove documentali di misure opportune ed efficaci per la realizzazione dei principi di protezione dei dati delineati nelle sezioni precedenti. Esempi di simili misure sono le procedure per garantire l'identificazione di tutte le operazioni di trattamento dei dati e per rispondere a richieste di accesso, la distribuzione di risorse tra cui la designazione di funzionari addetti alla protezione dei dati e responsabili dell'osservanza dei principi di protezione dei dati, ovvero procedure di certificazione indipendenti. Inoltre, i responsabili del trattamento dovrebbero garantire di essere pronti a

---

30 Cfr. sezione 3.4.2, punto 6 sopra. Il fornitore può anche ricevere istruzioni per rispondere a richieste a nome del cliente.

31 Preferibilmente, il fornitore dovrebbe utilizzare formati di dati e interfacce standard o aperti. In ogni caso, si dovrebbero concordare clausole contrattuali relative a formati garantiti, alla preservazione di relazioni logiche e a eventuali costi derivanti dalla migrazione ad un altro fornitore di servizi *cloud*.

dimostrare l'istituzione delle misure necessarie, su richiesta delle autorità di vigilanza competenti [32].

3.5 Trasferimenti internazionali

Gli articoli 25 e 26 della direttiva 95/46/CE prevedono il libero trasferimento di dati personali verso paesi extra-SEE solo se il paese o il destinatario garantisce un livello di protezione adeguato. Altrimenti, il responsabile del trattamento e i suoi corresponsabili e/o incaricati del trattamento sono tenuti a fornire garanzie specifiche. Tuttavia, il *cloud computing* si basa per lo più sulla completa mancanza di un'ubicazione stabile dei dati all'interno della rete del fornitore *cloud*. I dati possono trovarsi in un centro di trattamento alle 2 del pomeriggio e dall'altra parte del mondo alle 4 del pomeriggio. Il cliente *cloud* quindi è raramente nella posizione di sapere in tempo reale dove si trovano, dove sono archiviati o dove sono trasferiti i dati. In un simile contesto, gli strumenti giuridici tradizionali che fungono da quadro di riferimento per la regolamentazione dei trasferimenti di dati verso paesi terzi extra-UE che non forniscono una tutela adeguata, presentano delle limitazioni.

3.5.1 *Safe Harbor* e paesi adeguati

Gli accertamenti di adeguatezza, ivi compresi i principi *Safe Harbor* ("approdo sicuro"), hanno un ambito di applicazione geografica limitata e quindi non coprono tutti i trasferimenti all'interno del *cloud*.
I trasferimenti verso organizzazioni USA che aderiscono a tali principi possono avvenire legalmente ai sensi della legislazione UE, poiché si presume che le organizzazioni destinatarie forniscano un adeguato livello di protezione ai dati trasferiti.

Tuttavia, secondo il parere del Gruppo di lavoro, la sola autocertificazione di conformità al *Safe Harbor* può non essere considerata sufficiente in assenza di una solida applicazione dei principi di protezione dei dati nel contesto del sistema *cloud*. Inoltre, l'articolo 17 della direttiva UE prevede che il responsabile del trattamento stipuli un contratto con un incaricato ai fini del trattamento, come conferma la FAQ 10 dei documenti quadro dell'accordo *Safe Harbor* UE-USA. Il contratto non è soggetto alla preventiva autorizzazione delle autorità europee per la protezione dei dati (DPA) e specifica il trattamento da effettuare e eventuali misure necessarie per garantire che i dati siano mantenuti in sicurezza. Diverse legislazioni nazionali e DPA possono prevedere requisiti aggiuntivi.

Il Gruppo di lavoro ritiene che le società che esportano dati non dovrebbero semplicemente basarsi sulla dichiarazione dell'importatore dei dati in merito alla certificazione *Safe Harbor*. Al contrario, dovrebbero ottenere le prove dell'esistenza delle autocertificazioni *Safe Harbor* e richiedere che venga dimostrata l'osservanza dei relativi principi. Questo aspetto è importante, soprattutto per quanto concerne le informazioni fornite ai soggetti interessati dal trattamento dei dati[33, 34].

Il Gruppo di lavoro ritiene inoltre che il cliente *cloud* debba verificare se i contratti tipo offerti dai fornitori *cloud* siano conformi ai requisiti nazionali concernenti le clausole contrattuali sul trattamento dei dati. La legislazione nazionale può richiedere che nel contratto sia definito il subtrattamento, con la relative ubicazioni e i dati dei subincaricati, nonché la tracciabilità dei

---

[32] Il Gruppo di lavoro formula osservazioni dettagliate sull'argomento della responsabilità nel parere 3/2010 sul principio di responsabilità http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_it.pdf.

[33] Cfr. DPA tedesca: http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

[34] Per i requisiti concernenti i subincaricati, cfr. 3.3.2.

dati. Di norma, i fornitori *cloud* non forniscono simili informazioni al cliente; l'impegno nei confronti del *Safe Harbor* non può sostituire la mancanza delle garanzie di cui sopra, se richieste dalla legislazione nazionale. In questi casi, l'esportatore è incoraggiato a utilizzare altri strumenti giuridici disponibili, come le clausole contrattuali tipo o le norme vincolanti d'impresa (BCR).

Infine, il Gruppo di lavoro ritiene che i principi *Safe Harbor* di per se stessi non possano garantire all'esportatore dei dati gli strumenti necessari per assicurare che il fornitore di servizi *cloud* negli USA abbia applicato adeguate misure di sicurezza, come richiesto dalle legislazioni nazionali in base alla direttiva 95/46/CE[35]. In termini di sicurezza dei dati, il *cloud computing* comporta numerosi rischi specifici, quali la perdita di *governance*, l'insicurezza o incompletezza della cancellazione dei dati, piste di controllo (*audit trail*) insufficienti o carenze nell'isolamento[36], che non sono affrontati in misura sufficiente dai principi *Safe Harbor* esistenti in materia di sicurezza dei dati[37]. Occorre quindi prevedere garanzie aggiuntive per la sicurezza dei dati, ad esempio integrando competenze e risorse di terzi che siano in grado di valutare l'adeguatezza dei fornitori *cloud* con diversi sistemi di controllo, standardizzazione e certificazione[38]. Per questi motivi, sarebbe auspicabile integrare l'impegno dell'importatore di dati nei confronti del *Safe Harbor* con ulteriori garanzie che tengano conto della natura specifica dell'ambiente *cloud*.

3.5.2 Esenzioni

Le esenzioni previste all'articolo 26 della direttiva 95/46/CE consentono agli esportatori di dati di trasferire dati fuori dall'UE senza fornire garanzie aggiuntive. Tuttavia, il WP29 ha adottato un parere nel quale afferma che le esenzioni si applicano solo quando i trasferimenti non sono ricorrenti, né massicci o strutturali[39].

Sulla base di tali interpretazioni è quasi impossibile applicare delle deroghe nel contesto del *cloud computing*.

3.5.3 Clausole contrattuali tipo

Le clausole contrattuali tipo adottate dalla Commissione UE allo scopo di disciplinare i trasferimenti internazionali di dati tra due responsabili del trattamento o un responsabile e un incaricato del trattamento si basano su approccio bilaterale. Quando il fornitore *cloud* è considerato l'incaricato del trattamento, le clausole tipo come da decisione 2010/87/UE della Commissione sono uno strumento che l'incaricato e il responsabile del trattamento possono utilizzare come base per l'ambiente di *cloud computing*, per offrire garanzie adeguate nel contesto dei trasferimenti internazionali.

Oltre alle clausole contrattuali tipo, il Gruppo di lavoro ritiene che i fornitori di servizi *cloud* potrebbero offrire ai clienti disposizioni basate sulle loro esperienze concrete, nella misura in cui non contraddicano direttamente o indirettamente le clausole contrattuali tipo approvate

---

35 Cfr. un parere della DPA danese: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

36 Descritti in dettaglio nel documento ENISA *Cloud Computing: Benefits, Risks and Recommendations for Information Security* all'indirizzo: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

37 "Le organizzazioni devono prendere precauzioni ragionevoli per proteggere le informazioni personali da perdite, abusi e accesso non autorizzato, divulgazione, alterazione e distruzione".

38 Cfr. sezione 4.2 in appresso.

39 Documento di lavoro 12/1998: Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva UE sulla tutela dei dati, adottato dal Gruppo di lavoro il 24 luglio 1998 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_it.pdf).

dalla Commissione, né pregiudichino diritti e libertà fondamentali degli interessati[40]. In ogni caso, le società non possono modificare le clausole contrattuali tipo senza implicare che tali clausole non si possano più considerare "tipo"[41].

Quando il fornitore di servizi *cloud* che agisce in qualità di incaricato del trattamento è stabilito nell'UE, la situazione può rivelarsi più complessa poiché le clausole tipo si applicano, in generale, solo al trasferimento di dati da un responsabile del trattamento UE a un incaricato del trattamento non UE (cfr. considerando 23 della decisione 2010/87/UE della Commissione sulle clausole tipo e WP 176).

Per quanto concerne la relazione contrattuale tra l'incaricato del trattamento non UE e i subincaricati, dovrebbe esistere un accordo scritto che imponga ai subincaricati gli stessi obblighi imposti all'incaricato del trattamento nelle clausole tipo.

3.5.4 Norme vincolanti d'impresa (BCR): verso un approccio globale

Le BCR costituiscono un codice di condotta per le società che trasferiscono dati all'interno del proprio gruppo. Si tratta di una soluzione applicabile anche nel contesto del *cloud computing* quando il fornitore del servizio è un incaricato del trattamento. In effetti, il WP29 attualmente sta lavorando su BCR per incaricati del trattamento, che consentano il trasferimento all'interno del gruppo a vantaggio dei responsabili del trattamento senza richiedere la firma di un contratto tra incaricato del trattamento e subincaricati per ciascun cliente[42].

Questo tipo di BCR per gli incaricati del trattamento consentirebbero al cliente di affidare i propri dati personali all'incaricato del trattamento con la sicurezza che i dati trasferiti entro la portata dell'attività del fornitore del servizio ricevano un adeguato livello di protezione.

4. Conclusioni e raccomandazioni

Imprese e amministrazioni che intendono ricorrere al *cloud computing* dovrebbero effettuare per prima cosa un'analisi del rischio completa e approfondita, prendendo in esame i rischi relativi al trattamento dei dati nel sistema *cloud* (scarso controllo e informazioni insufficienti – cfr. sezione 2 che precede) con riferimento alla tipologia di dati trattati nel *cloud*[43]. Inoltre, si dovrebbe prestare un'attenzione particolare alla valutazione dei rischi legali in materia di protezione dei dati, che riguardano principalmente obblighi di sicurezza e trasferimenti internazionali. Il trattamento di dati sensibili via *cloud computing* solleva ulteriori preoccupazioni. Per questo, fatte salve le leggi nazionali, tale trattamento richiede garanzie aggiuntive[44]. Le conclusioni che seguono sono intese a fornire una lista di controllo per l'osservanza dei principi di protezione dei dati da parte di clienti e fornitori di servizi *cloud*

---

40 Cfr. FAQ IV B1.9 9, Le società possono includere le clausole contrattuali tipo in un contratto più ampio e aggiungere clausole specifiche?, pubblicata dalla CE all'indirizzo http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

41 Cfr. FAQ IV B1.10, Le società possono modificare le clausole contrattuali tipo approvate dalla Commissione?

42 Cfr. documento di lavoro 02/2012, contenente una tabella con gli elementi e i principi da prevedere nelle norme vincolanti d'impresa (BCR) dell'incaricato del trattamento, adottato il 6 giugno 2012: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

43 ENISA presenta un elenco dei rischi da prendere in considerazione http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

44 Cfr. Memorandum di Sopot, nota 2 che precede.

sulla base dell'attuale quadro giuridico; vengono fornite anche una serie di raccomandazioni in vista dei futuri sviluppi nel quadro normativo a livello UE e internazionale.

4.1 Linee guida per clienti e fornitori di servizi di cloud computing

- Relazione responsabile del trattamento-incaricato del trattamento: il presente parere si incentra sulla relazione cliente-fornitore in quanto relazione tra responsabile del trattamento e incaricato del trattamento (cfr. sezione 3.3.1). In ogni caso, sulla base di circostanze concrete possono esistere situazioni dove il fornitore *cloud* agisce anche da responsabile del trattamento, ad esempio quando procede all'ulteriore trattamento di dati personali per scopri propri. In tal caso, il fornitore *cloud* ha la piena responsabilità (congiunta) del trattamento ed è tenuto ad adempiere a tutti gli obblighi di legge sanciti dalle direttive 95/46/CE e 2002/58/CE (se pertinente).
- Responsabilità del cliente *cloud* in quanto responsabile del trattamento: il cliente in quanto responsabile del trattamento deve assumere la responsabilità di attenersi alla legislazione sulla protezione dei dati ed è soggetto a tutti gli obblighi di legge di cui alle direttive 95/46/CE e 2002/58/CE, se pertinente, in particolare nei confronti degli interessati (cfr. 3.3.1). Il cliente dovrebbe scegliere un fornitore *cloud* che garantisca la conformità con la legislazione UE in materia di protezione dei dati, rispecchiata dalle adeguate garanzie contrattuali sintetizzate in appresso.
- Garanzie relative ai subcontraenti: qualsiasi contratto tra fornitore e cliente di servizi *cloud* dovrebbe prevedere delle clausole relative ai subcontraenti. Il contratto dovrebbe specificare che i subincaricati possono essere autorizzati solo sulla base di un consenso che di norma può essere concesso dal responsabile del trattamento a fronte di un chiaro obbligo dell'incaricato del trattamento di informarlo in merito a eventuali cambiamenti previsti in proposito, mentre il responsabile del trattamento si riserva la possibilità, in qualsiasi momento, di opporsi a tali cambiamenti o di risolvere il contratto. Il contratto dovrebbe chiarire l'obbligo del fornitore *cloud* di indicare tutti i subcontraenti autorizzati. Inoltre, il fornitore *cloud* è tenuto a stipulare un contratto con ciascun subcontraente che rispecchi le clausole del contratto stipulato con il cliente *cloud*; il cliente dovrebbe garantire di essere in grado di avvalersi di possibilità di ricorso in caso di violazioni dei contratti da parte dei subcontraenti del fornitore (cfr. 3.3.2).
- Osservanza dei principi fondamentali in materia di protezione dei dati:
    - Trasparenza (cfr. 3.4.1.1): i fornitori *cloud* dovrebbero informare i clienti *cloud* in merito a tutti gli aspetti pertinenti (per la protezione dei dati) dei propri servizi durante i negoziati per il contratto; in particolare, i clienti dovrebbero essere informati in merito a tutti i subcontraenti che contribuiscono alla prestazione dei rispettivi servizi *cloud* e a tutte le sedi presso le quali i dati possono essere archiviati o trattati dal fornitore *cloud* e/o dai suoi subcontraenti (in particolare se alcune o tutte le sedi si trovano fuori dello Spazio economico europeo, SEE); il cliente dovrebbe ricevere informazioni significative in merito a misure tecniche e organizzative attuate dal fornitore; a titolo di buona prassi, il cliente dovrebbe informare gli interessati in merito al fornitore di servizi *cloud* e a tutti i subcontraenti (eventuali) nonché in merito alle sedi presso le quali i dati possono essere conservati o trattati dal fornitore *cloud* e/o dai suoi subcontraenti;
    - Specificazione e limitazione della finalità (3.4.1.2): il cliente dovrebbe garantire l'osservanza dei principi di specificazione e limitazione della finalità

e assicurare che il fornitore di servizi o eventuali subcontraenti non procedano al trattamento di dati per finalità diverse. L'impegno a tale proposito dovrebbe essere contenuto in opportune disposizioni contrattuali (ivi comprese garanzie tecniche e organizzative);

- Conservazione dei dati (3.4.1.3): i cliente ha la responsabilità di garantire che i dati personali vengano cancellati (dal fornitore del servizio e da eventuali subcontraenti) da qualsiasi supporto sul quale siano memorizzati, non appena non sono più necessari per gli scopi specificati; il contratto dovrebbe prevedere meccanismi sicuri di cancellazione (distruzione, smagnetizzazione, sovrascrittura).

- Garanzie contrattuali (cfr. 3.4.2, 3.4.3 e 3.5):

  - In generale: il contratto con il fornitore di servizi (e quelli stipulati tra fornitore e subcontraenti) dovrebbe fornire garanzie sufficienti in termini di sicurezza tecnica e misure organizzative (a norma dell'articolo 17, paragrafo 2, della direttiva) ed essere in forma scritta o in un'altra forma equivalente. Il contratto dovrebbe descrivere nel dettaglio le istruzioni del cliente al fornitore del servizio, tra cui oggetto e orizzonte temporale del servizio, accordi sul livello del servizio (SLA) oggettivi e misurabili, nonché le sanzioni pertinenti (finanziarie o altro); inoltre dovrebbe specificare le misure di sicurezza da rispettare in funzione dei rischi del trattamento e della natura dei dati, in linea con i requisiti indicati in appresso e ferma restando l'applicazione di eventuali misure più rigorose previste dalla legislazione nazionale del cliente; se i fornitori *cloud* intendono utilizzare condizioni contrattuali tipo, dovrebbero garantire che tali condizioni siano conformi ai requisiti in materia di protezione dei dati (cfr. 3.4.2); in particolare, le rispettive condizioni dovrebbero specificare le misure tecniche e organizzative attuate dal fornitore del servizio.

  - Accesso ai dati: solo le persone autorizzate dovrebbero avere accesso ai dati; nel contratto si dovrebbe inserire una clausola di riservatezza vincolante per il fornitore di servizi *cloud* e per i suoi dipendenti.

  - Divulgazione dei dati a terzi: questo aspetto dovrebbe essere disciplinato solo dal contratto, che dovrebbe prevedere l'obbligo per il fornitore del servizio di indicare tutti i subcontraenti, ad esempio in un registro digitale pubblico, e garantire al cliente l'accesso a informazioni relative a eventuali cambiamenti, che gli consentano di opporsi a tali cambiamenti o di risolvere il contratto; inoltre, ai sensi del contratto il fornitore dovrebbe essere tenuto a comunicare eventuali richieste legalmente vincolanti di divulgazione di dati personali da parte di un'autorità giudiziaria o di polizia, a meno che tale divulgazione sia comunque vietata; il cliente dovrebbe garantire che il fornitore respinga eventuali richieste di divulgazione non legalmente vincolanti.

  - Obbligo di cooperare: il cliente dovrebbe garantire che il fornitore sia obbligato a cooperare in merito al diritto del cliente di controllare le operazioni di trattamento, agevolare l'esercizio dei diritti degli interessati ad accedere/rettificare/cancellare i loro dati e (se pertinente) comunicare al cliente *cloud* eventuali violazioni concernenti i dati del cliente.

  - Trasferimenti transfrontalieri di dati: il cliente *cloud* dovrebbe verificare se il fornitore *cloud* è in grado di garantire la legittimità dei trasferimenti transfrontalieri di dati e se possibile limitare i trasferimenti a paesi selezionati dal cliente. I trasferimenti di dati a paesi terzi non adeguati richiedono garanzie

specifiche, tramite il ricorso ad accordi *Safe Harbor*, clausole contrattuali tipo o norme vincolanti d'impresa (BCR) se del caso; l'utilizzo di clausole contrattuali tipo per gli incaricati del trattamento (a norma della decisione n. 2010/87/CE della Commissione) richiede determinati adeguamenti per l'ambiente *cloud* (per evitare la stipulazione di contratti separati per cliente tra un fornitore di servizi e i suoi subincaricati) che potrebbero comportare la necessità di autorizzazioni preventive dalla DPA competente; il contratto dovrebbe comprendere un elenco dei luoghi dove potrebbe essere fornito il servizio.

- *Logging* e *auditing* del trattamento: il cliente dovrebbe richiedere la registrazione (*logging*) delle operazioni di trattamento eseguite dal fornitore e dai suoi subcontraenti; il cliente dovrebbe essere autorizzato a effettuare l'*audit* di tali operazioni di trattamento, benché siano accettabili anche *audit* e certificazioni di terzi scelti dal responsabile del trattamento, purché sia garantita la piena trasparenza (ad es. prevedendo la possibilità di ottenere una copia del certificato di *audit* o una copia della relazione di *audit* che verifica la certificazione).
- Misure tecniche e organizzative: dovrebbero essere mirate a porre rimedio ai rischi comportati dalla mancanza di controllo e di informazioni che caratterizzano in misura rilevante l'ambiente di *cloud computing*. Le prime comprendono misure mirate a garantire disponibilità, integrità, riservatezza, isolamento, possibilità di intervento e portabilità, come definiti nel documento, mentre le secondo sono incentrate sulla trasparenza (cfr. 3.4.3 per i dettagli completi).

4.2 Certificazioni di terzi sulla protezione dei dati

- La verifica o la certificazione indipendente effettuata da un terzo affidabile può essere uno strumento credibile per i fornitori *cloud* per dimostrare la conformità con gli obblighi posti a loro carico, come specificato nel presente parere. Una simile certificazione indicherebbe come minimo che i controlli in materia di protezione dei dati sono stati oggetto di *audit* o verifica a fronte di una norma riconosciuta e conforme ai requisiti indicati nel presente parere, stabilita da un'organizzazione terza rispettabile[45]. Nel contesto del *cloud computing*, i potenziali clienti dovrebbero cercare di capire se i fornitori *cloud* possono fornire una copia della certificazione di terzi o una copia della relazione di *audit* che attesti la certificazione anche rispetto ai requisiti esposti nel presente parere.
- Singoli *audit* di dati ospitati in un *server* plurimo e virtuale possono essere tecnicamente impraticabili e in alcuni casi possono servire ad aumentare i rischi per i controlli di sicurezza esistenti sulla rete fisica e logica. In questi casi, un *audit* effettuato da un terzo scelto dal responsabile del trattamento può essere ritenuta soddisfacente in luogo del diritto all'*audit* del singolo responsabile del trattamento.
- L'adozione di norme e certificazioni specifiche per la privacy è cruciale per l'istituzione di un rapporto di fiducia tra fornitori *cloud*, responsabili del trattamento e persone interessate.

[45] Tali norme comprenderebbero quelle emesse dall'International Standards Organisation, dall'International Auditing and Assurance Standards Board e dall'Auditing Standards Board of the American Institute of Certified Public Accountants nella misura in cui queste organizzazioni emettono norme rispondenti ai requisiti esposti nel presente parere.

- Queste norme e certificazioni dovrebbero prendere in considerazione misure tecniche (quali ubicazione dei dati o criptaggio) nonché procedure all'interno dell'organizzazione del fornitore *cloud* che garantiscano la protezione dei dati (quali politiche di controllo dell'accesso, controllo dell'accesso o *backup*).

4.3 Raccomandazioni: sviluppi futuri

Il Gruppo di lavoro articolo 29 è pienamente consapevole del fatto che la complessità del *cloud computing* non può essere affrontata completamente attraverso le garanzie e le soluzioni delineate nel presente parere, che tuttavia offre una solida base per garantire il trattamento di dati personali sottoposti a fornitori *cloud* da clienti con sede nel SEE. La presente sezione è intesa a evidenziare alcune questioni che devono essere affrontate nel breve-medio termine per rafforzare le garanzie già in essere, assistendo il settore del *cloud computing* con riferimento alle problematiche evidenziate nel garantire il rispetto dei diritti fondamentali alla privacy e alla protezione dei dati.

- Maggiore equilibrio di responsabilità tra responsabile e incaricato del trattamento: il Gruppo di lavoro articolo 29 apprezza le disposizioni dell'articolo 26 della proposta della Commissione (progetto di regolamento generale UE sulla protezione dei dati) mirate ad aumentare la responsabilità degli incaricati del trattamento nei confronti dei responsabili del trattamento, assistendoli nel garantire la conformità in particolare con i requisiti di sicurezza e i relativi obblighi. L'articolo 30 della proposta introduce l'obbligo legale per l'incaricato del trattamento di adottare adeguate misure tecniche e organizzative. Il progetto di proposta chiarisce che un incaricato che non si attiene alle istruzioni del responsabile del trattamento è considerato responsabile del trattamento ed è soggetto alle norme specifiche sui corresponsabili del trattamento. Il Gruppo di lavoro articolo 29 ritiene che la proposta vada nella giusta direzione per porre rimedio allo squilibrio che spesso caratterizza l'ambiente del *cloud computing*, dove il cliente (in particolare se si tratta di una PMI) può incontrare difficoltà ad esercitare il pieno controllo richiesto dalla legislazione sulla protezione dei dati in merito alle modalità di fornitura dei servizi richiesti. Inoltre, in considerazione della posizione giuridica asimmetrica degli interessati e degli utenti piccole imprese nei confronti dei grandi fornitori di servizi di *cloud computing*, si raccomanda un ruolo più proattivo delle organizzazioni di consumatori e imprese per negoziare termini e condizioni generali più equilibrati.

- Accesso ai dati personali per motivi di sicurezza nazionale e attività di contrasto: è della massima importanza aggiungere al futuro regolamento una disposizione che vieti ai responsabili del trattamento operanti nell'UE di divulgare dati personali ad un paese terzo su richiesta dell'autorità giudiziaria o amministrativa di tale paese terzo, salvo espressa autorizzazione prevista da un accordo internazionale o da trattati di mutua assistenza legale o approvata da un'autorità di vigilanza. Il regolamento (CE) n. 2271/96 del Consiglio è un esempio appropriato di base giuridica per questo aspetto[46]. Il Gruppo di lavoro è preoccupato per questa lacuna nella proposta della Commissione, poiché comporta una considerevole perdita di certezza giuridica per gli interessati i cui dati personali sono memorizzati in centri di trattamento dati in tutto il mondo. Per questo motivo, il Gruppo di lavoro sottolinea[47] la necessità di includere nel regolamento l'uso

[46] Regolamento (CE) n. 2271/96 del Consiglio del 22 novembre 1996 relativo alla protezione dagli effetti extraterritoriali derivanti dall'applicazione della normativa adottata da un paese terzo, e dalle azioni su di essa basate o da essa derivanti, Gazzetta Ufficiale L 309 del 29/11/1996, pagg. 0001 - 0006, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:IT:HTML

[47] Cfr. WP 191 - Parere 01/2012 sulle proposte di riforma della protezione dei dati, pag. 23.

obbligatorio di trattati di assistenza giuridica reciproca (MLAT) in caso di divulgazioni non autorizzate dalla legge dell'Unione o di Stati membri.

- Precauzioni particolari del settore pubblico: occorre aggiungere un *caveat* particolare in merito alla necessità che un ente pubblico valuti innanzi tutto se la comunicazione, il trattamento e la conservazione di dati fuori dal territorio nazionale possa esporre a rischi inaccettabili la sicurezza e la privacy dei cittadini, nonché la sicurezza e l'economia nazionale, in particolare se sono coinvolte banche dati sensibili (ad es. dati del censimento) e servizi (ad es. servizi sanitari)[48]. Questa speciale considerazione andrebbe prestata comunque, ogniqualvolta si trattino dati sensibili in un contesto *cloud*. Da questo punto di vista, i governi nazionali e le istituzioni dell'Unione europea potrebbero considerare di approfondire ulteriormente il concetto di *cloud computing* governativo europeo in quanto spazio virtuale sovranazionale dove si potrebbero applicare una serie di regole coerenti e armonizzate.

- *European Cloud Partnership* (Partenariato europeo per il cloud): il Gruppo di lavoro articolo 29 sostiene la strategia *European Cloud Partnership* (ECP) presentata dalla Commissaria Kroes, Vicepresidente della Commissione europea, nel gennaio 2012 a Davos[49]. La strategia prevede appalti pubblici per tecnologie informatiche al fine di stimolare un mercato europeo del *cloud computing*. Il trasferimento di dati personali a un fornitore europeo di servizi *cloud*, disciplinato autonomamente dalla legge europea sulla protezione dei dati, potrebbe portare grandi vantaggi ai clienti in fatto di protezione dei dati, in particolare promuovendo l'adozione di norme comuni (specialmente in termini di interoperabilità e portabilità dei dati), nonché la certezza giuridica.

---

48 A questo proposito, ENISA formula la seguente raccomandazione nel suo documento su sicurezza e resilienza in *cloud* governativi (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): "In termini di architettura, per applicazioni sensibili le soluzioni *cloud* private e di comunità sembrano essere quelle che attualmente rispondono meglio alle esigenze delle pubbliche amministrazioni perché offrono il massimo livello di governance, controllo e visibilità, anche se nel pianificare un sistema *cloud* privato o di comunità si dovrebbe prendere in particolare considerazione la scala dell'infrastruttura".

49 Neelie Kroes, Vicepresidente della Commissione europea responsabile per l'Agenda digitale, *Setting up the European Cloud Partnership*, World Economic Forum Davos, Svizzera, 26 gennaio 2012, URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ALLEGATO

a) Modelli di rollout

Un ***private cloud***[50] è un'infrastruttura informatica dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo (nella tradizionale forma dell'*hosting* dei *server*) nei confronti del quale il responsabile del trattamento esercita un controllo puntuale. Il *private cloud* si può paragonare a un tradizionale centro di trattamento dati (*data center*), con la differenza che, grazie a degli accorgimenti tecnologici, è possibile ottimizzare l'utilizzo delle risorse disponibili e potenziarle attraverso investimenti contenuti e attuati progressivamente nel tempo.

Nel caso dei ***public cloud***, invece, l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o pubbliche amministrazioni - e quindi condivide tra di essi - i propri sistemi. La fruizione di tali servizi avviene tramite la rete Internet e implica il trasferimento delle operazioni di trattamento dei dati e/o dei soli dati ai sistemi del fornitore del servizio, il quale assume pertanto un ruolo importante in ordine all'efficacia della protezione dei dati che gli sono stati affidati. Insieme ai dati, l'utente cede una parte importante del controllo esercitabile su di essi.

Accanto ai *private* e *public cloud* si annoverano i cosiddetti *cloud* "intermedi" o "ibridi", dove i servizi erogati da infrastrutture private coesistono con servizi acquisiti da *cloud* pubblici. Vanno citati anche i *community cloud* (o *cloud* di comunità) in cui l'infrastruttura informatica è condivisa da diverse organizzazioni a beneficio di una specifica comunità di utenti.

La flessibilità e la semplicità con cui è possibile configurare i sistemi in *cloud* ne rende possibile un dimensionamento "elastico", ossia adeguato alle esigenze specifiche secondo un approccio basato sull'utilizzo. Gli utenti non devono curarsi della gestione dei sistemi informatici che, essendo utilizzati sulla base di accordi di esternalizzazione (*outsourcing*), sono completamente gestiti dai soggetti terzi nel cui *cloud* sono conservati i dati. Spesso entrano in gioco fornitori di grosse dimensioni dotati di infrastrutture complesse, e per questo motivo il *cloud* può estendersi geograficamente in numerosi luoghi distinti e gli utenti potrebbero ignorare dove vengono effettivamente conservati i loro dati.

---

[50] Il NIST (National Institute of Standards and Technology) negli USA ha lavorato per qualche anno sulla standardizzazione delle tecnologie basate sul *cloud* e anche il documento di ENISA fa riferimento alle sue definizioni:
Private cloud.
L'infrastruttura *cloud* è dedicata esclusivamente a un'organizzazione. Può essere gestita dall'organizzazione stessa o da un terzo e può esistere in sede o altrove. Va notato che un *private cloud* si basa almeno su determinate tecnologie che sono tipiche anche dei *public cloud* – tra cui, in particolare, tecnologie di virtualizzazione che promuovono la riorganizzazione (o revisione) dell'architettura del trattamento dati come spiegato sopra.
Public cloud.
L'infrastruttura cloud è resa disponibile al pubblico in generale o a un grande gruppo industriale ed è di proprietà di un'organizzazione che vende servizi *cloud*.

b) Modelli di erogazione dei servizi

A seconda delle esigenze dell'utente, sul mercato sono disponibili varie soluzioni di *cloud computing*, che ricadono in linea di massima in tre categorie, o "modelli di servizio". Di norma, tali modelli sono riferiti sia a soluzioni di *private cloud* che di *public cloud*:

- **IaaS (*Cloud Infrastructure as a Service*)** (infrastruttura *cloud* resa disponibile come servizio): il fornitore noleggia un'infrastruttura tecnologica, cioè *server* virtuali remoti che l'utente finale può utilizzare con tecniche e modalità che rendono semplice, efficace e vantaggioso sostituire i sistemi informatici aziendali presenti nei locali dell'azienda e/o affiancare l'infrastruttura noleggiata ai sistemi aziendali. Tali fornitori sono in genere operatori di mercato specializzati, che realmente dispongono di un'infrastruttura fisica complessa, spesso distribuita in aree geografiche diverse.

- **SaaS (*Cloud Software as a Service*)** (software erogato come servizio *cloud*)**:** un fornitore eroga via web una serie di servizi applicativi mettendoli a disposizione degli utenti finali. Questi servizi sono spesso offerti in sostituzione delle tradizionali applicazioni installate localmente dall'utente sui propri sistemi; di conseguenza, l'utente è spinto a esternalizzare i suoi dati affidandoli al singolo fornitore. Si pensi, ad esempio, ad applicazioni tipiche per l'ufficio erogate in modalità web quali fogli di calcolo, strumenti di elaborazione testi, registri e agende computerizzati, calendari condivisi, ecc., ma anche a servizi come le applicazioni di posta elettronica *cloud*.
- **PaaS (*Cloud Platform as a Service*)** (piattaforme *cloud* fornite via web come servizio): il fornitore offre soluzioni per lo sviluppo e l'*hosting* evoluto di applicazioni. In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie, allo scopo di soddisfare esigenze interne e/o per fornire a loro volta servizi a terzi. Anche nel caso del PaaS il servizio erogato dal fornitore elimina la necessità per l'utente di doversi dotare internamente di strumenti *hardware* o *software* specifici o aggiuntivi.

Una transizione completa ad un sistema *cloud* totalmente pubblico non sembra fattibile nel breve periodo per una serie di motivi, in particolare per quanto concerne entità di notevoli dimensioni come grandi aziende o organizzazioni che devono adempiere a obblighi specifici, quali le maggiori banche, enti governativi, grandi municipalità, ecc. Questo si può spiegare principalmente per due motivi: innanzi tutto, esiste un fattore di slancio relativo agli investimenti richiesti per realizzare una simile transizione; in secondo luogo, occorre tenere conto delle informazioni particolarmente preziose e/o delicate da trattare in casi specifici.

Un altro fattore a favore dei *private cloud* (almeno nei casi citati sopra) è il fatto che i fornitori di *public cloud* spesso non sono in grado di garantire una qualità del servizio (sulla base di accordi sul livello del servizio) tale da stare al passo con la natura delicata del servizio che deve erogare il responsabile del trattamento, a volte perché larghezza di banda e affidabilità della rete non sono sufficienti o adeguate in una data area, o anche per quanto riguarda specifiche connessioni utente-fornitore. D'altro canto, si può ragionevolmente presumere che in alcuni dei casi sopra citati si possano affittare o noleggiare *private cloud* (perché può essere una soluzione più efficiente in termini di costo) o si possano utilizzare modelli di *cloud* ibridi (che comprendono componenti pubbliche e private). In tutti i casi occorre valutare attentamente tutte le implicazioni pertinenti.

In assenza di norme concordate a livello internazionale, esiste il rischio di soluzioni *cloud* "fai da te", o anche federate, che comportano maggiori pericoli di *lock-in* (oltre a quelle che sono

state definite "monocolture della privacy")[51] e impediscono il pieno controllo sui dati senza garantire l'interoperabilità. In effetti, interoperabilità e portabilità dei dati sono fattori chiave per lo sviluppo di una tecnologia *cloud* e per consentire il pieno esercizio dei diritti di protezione dei dati degli interessati (quali l'accesso o la rettifica).

Da questo punto di vista, l'attuale dibattito sulle tecnologie *cloud* offre un esempio significativo della tensione esistente tra approcci orientati ai costi e orientati ai diritti, come descritto in breve nella sezione 2 che precede. Basarsi sui *private cloud* può essere fattibile e addirittura consigliabile in una prospettiva di protezione dei dati, tenendo conto delle circostanze specifiche del trattamento, ma nel lungo termine si può dimostrare impraticabile per le organizzazioni, soprattutto in un prospettiva orientata ai costi. Occorre un'attenta valutazione degli interessi in gioco, perché attualmente in questo campo non è possibile indicare una soluzione univoca.

[51] Cfr. lo studio del Parlamento europeo *Does it Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy*, pubblicato nel dicembre 2011.