ISSN: 2281-5147

Opinio Juris in Comparatione

Studies in Comparative and National Law

Op. J. Vol. I, n. I/2015

I Soggetti Coinvolti nel Trattamento dei Dati Personali nel Cloud Computing: la Rottura del Dualismo *Controller-Processor*

by

Gianclaudio Malgieri

www.opiniojurisincomparatione.org

I SOGGETTI COINVOLTI NEL TRATTAMENTO DEI DATI PERSONALI NEL *CLOUD COMPUTING*: LA ROTTURA DEL DUALISMO *CONTROLLER-PROCESSOR*

by

Gianclaudio Malgieri[*]

Abstract:

The current data protection directive is inadequate to cope with the complexity of the technology of cloud computing. However, the Proposed General Data Protection Regulation seems to offer a suitable solution to this problem.

The main issue is to establish who is the controller, and who is the processor in the cloud computing data processing, even considering all intermediate or subordinate positions and the two different kinds of data: *user-related* personal information and *cloud-processed* personal information.

Several asymmetries complicate this qualification: a contractual and a structural asymmetry does not allow the "user" to be defined a data-controller, in fact, although he determines "scope" and "means" of the treatment, he is a mere "cloud consumer" (users ignore individuals involved in the treatment, the location of the servers where data are collected, and their displacement; he can neither determine autonomously technical or security means of the processing and he just accepts a standard contract). On the other side, an information asymmetry does not allow the "provider" to be defined a data-processor (providers accesses to data just incidentally and just for technical purposes and usually fragments data so that they are not intelligible as personal data). Moreover, if the user is proved to be the "controller" he would be covered by the "*household exemption*", with the paradox that the only subject which would be legally liable is the provider-processor (whose role depends on the decisions of the controller).

This context is further complicated by the more and more diffused practice to outsource the cloud providing service to sub-contractors ("*sub-processors*").

Fortunately, the Proposed Regulation can provide a general solution to these problems by the new figure of the "*joint-controller" (art. 24)* and the more onerous figure of the processor (with precise requirements for the "sub-processor").

This paper proposes to break the dualism controller/processor and espouse a multi-level, transverse and functionalist approach: so for cloud-processed data, the user would be a "subject/joint-controller", the provider a "processor/joint-controller". In fact, the purposes of the processing are mainly determined by the users; while conditions and technical means are determined by the provider and the choice of security means is shared. It is also interesting to underlined that the Proposed Regulation specifies that processors who processes data beyond the controller's instructions is to be considered as a joint controller (art. 26).

Obviously, the breach of dualism controller/processor requires precise and accurate Terms of Use. From a general review of the terms of use of several popular cloud services, none of them defines precisely the role of provider. The most desirable solution would be the development of a European standard for privacy terms clarifying the different functions, responsibilities, rights and duties for all different subjects involved in a cloud service.

Keywords: joint controller - data controller - data processor - sub-processor - cloud computing – privacy - Data Protection Regulation - cloud provider - cloud consumer - cloud user.

---

[*] Gianclaudio Malgieri is undergraduate law student at Sant'Anna School of Advanced Studies in Pisa.

TABLE OF CONTENTS

I. INTRODUZIONE

La disciplina europea sul trattamento dei dati personali[1] trova non pochi problemi applicativi nello sviluppo di nuove infrastrutture tecnologiche, tra cui *in primis* il *cloud computing*, rivoluzione degli ultimi anni che sembra cambiare definitivamente il modo di concepire l'uso della tecnologia e i mezzi di gestione delle informazioni.

Un problema che appare primario nell' impiego delle tecnologie di *cloud* è la definizione dei ruoli e delle qualifiche giuridiche per l'utilizzo e il trattamento dei dati personali.

La specifica struttura del *cloud computing*, infatti, e le successive soluzioni organizzative del mercato (*outsourcing*, sub-contratti, ecc.), rendono di non facile identificazione il confine tra *controller* e *processor* dei dati personali, cioè tra responsabile ed incaricato del trattamento, e conseguentemente la disciplina della responsabilità, ai sensi della direttiva 95/46/CE, con le relative leggi di applicazione nazionale.

A risolvere in parte i problemi di definizione di qualifiche e scopi nel mondo del *cloud* (lasciando tuttavia aree ancora irrisolte) interverrà a breve il Regolamento Generale sul Trattamento dei Dati Personali[2], ancora da approvare definitivamente (da qui in avanti: *Proposed Regulation*).

Per ragioni di chiarezza occorre prima effettuare una ricognizione generale delle qualifiche dei soggetti che effettuano il trattamento dei dati alla luce della normativa europea, vigente e futura.

In seguito, si cercherà di verificare l'impatto di tale disciplina sugli operatori del *cloud computing*, appurando in che misura l'utente di un servizio *cloud* sia un *controller* o un mero "interessato" del trattamento, e come si declini il ruolo del *cloud provider*: *non-processor*, *processor*, *controller*, o piuttosto "*joint controller*".

Per un'analisi corretta occorrerà distinguere concretamente i tipi di dati nella disponibilità dei fornitori di servizi *cloud*: dati collegati al profilo dell'utente (*user-related personal data*) e dati immagazzinati per volontà dell'utente (*cloud-processed personal data*).

Occorrerà poi distinguere le diverse tipologie infrastrutturali in cui si declina il *cloud computing*: da mere infrastrutture (*IaaS*) a software (*SaaS*), da piattaforme per il *mass storage* a strutture complesse come i *social network*.

II. IL DATO NORMATIVO: LA DEFINIZIONE TEORICA DI CONTROLLER E PROCESSOR TRA LA DIRETTIVA 95/46/CE E IL FUTURO REGOLAMENTO

La direttiva 95/46/CE definisce il *controller* all'art. 2, lett. D: "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 di dati personali".

La disciplina di attuazione nazionale della direttiva, inoltre, specifica che nella determinazione degli strumenti del trattamento richiesta al *controller* si deve intendere anche un altro requisito: il "profilo della sicurezza" (art. 4, comma 1, lett. f e art. 28 del Codice in materia di protezione dei dati personali[3]). In più, la *Proposed Regulation* menziona anche le "condizioni" del trattamento (art. 4, n. 5).

Per "finalità" bisogna intendersi gli obiettivi e gli scopi per cui si effettua il trattamento, al contrario le "modalità" o gli "strumenti" (o i "mezzi" come afferma la *Proposed Regulation*) riguardano le concrete caratteristiche del trattamento (qualità dei dati da trattare, soggetti a cui comunicarli). I "profili

[1] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[2] Risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla 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 (regolamento generale sulla protezione dei dati) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

[3] D.lgs. 30 giugno 2003 n. 196 o Codice in materia di protezione dei dati personali (di qui in avanti: codice della privacy).

di sicurezza", invece, attengono alle misure attraverso cui garantire salvaguardia dei dati da possibili distruzioni o perdite, accessi o usi non consentiti.[4]

Tuttavia, si è fatto notare come le differenti definizioni dei compiti del *controller* non comporti effettive differenze, dato che le "modalità" appaiono espressione generale, che come tale può essere comprensiva anche degli strumenti del trattamento, e dall'altra l'adozione di qualsiasi strumento finisce per incidere sulle modalità del trattamento.[5]

Il *processor*, invece, è "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento" (art. 2, lett. F della direttiva 95/46/CE).

Innanzitutto è bene sottolineare una differenza terminologica tra la disciplina europea e quella italiana.

Controller è tradotto, nella versione italiana della direttiva, come "responsabile" e *processor* come "incaricato".

Al contrario, nella legge di attuazione italiana[6] si utilizza il termine "titolare" per indicare il responsabile, "responsabile" è invece il *processor*-incaricato, e "incaricato" la eventuale terza persona[7] che effettua materialmente il trattamento.

La traslazione lessicale, tuttavia, se sembra spostare la responsabilità dal *controller* al *processor* (poiché "responsabile" non è più denominato il primo, ma il secondo), nei fatti non comporta differenze giuridiche rilevanti.[8]

Di qui in avanti si preferirà la dizione inglese dei ruoli (*controller* e *processor*) per evitare confusione e per seguire un approccio europeo rispetto ai concetti in esame.

Il dato rilevante, ai fini di tale articolo, è lo stretto rapporto tra *controller* e *processor*. Un rapporto di dipendenza funzionale del secondo al primo: mentre il *controller* esiste in quanto soggetto che determina in piena autonomia le finalità, gli strumenti e le misure di sicurezza per il trattamento dei dati personali, il *processor*, invece, esiste se e in quanto nominato dal *controller* come esecutore materiale di quegli strumenti e di quelle misure di sicurezza determinati dal *controller*.[9]

Egli, inoltre, deve essere scelto tra coloro che ("per esperienza, capacità ed affidabilità"[10]) mostrano garanzie sufficienti per mettere in atto misure di sicurezza tecnica ed organizzativa dei dati nel rispetto dei vincoli della normativa.[11]

Il *processor* può anche coincidere col *controller* e tuttavia non è un mero esecutore privo di autonomia. Al contrario, la delega implica un certo grado di discrezionalità riguardo al come servire al meglio gli interessi del *controller*, permettendo al *processor* di scegliere la tecnica e le misure organizzative più adatte,[12] conformemente alla lettera del mandato.[13]

---

[4] C. DI COCCO, *Soggetti che effettuano il trattamento,* in *Il codice in materia di protezione dei dati personali, Commentario sistematico al d.lgs. 30 giugno 2003 n.196,* a cura di J. Monducci e G. Sartor., Padova, 2004, 123.

[5] P.M. VECCHI, *Art. 4 - Definizioni*, in *La protezione dei dati personali*, *Commentario al D.Lgs. 30 giugno 2003, n. 196 «Codice della privacy»,* in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali, Commentario al D.lgs. 30 giugno 2003, n. 196*, Tomo I, Padova, 2007, 69.

[6] Art. 2, comma 1, lett. d-f e artt. 7 e 8 della legge del 31 dicembre 1996, n. 675 trasposti poi nell'art. 4, comma 1, lett. f-i e negli artt. 28-30, cod. privacy.

[7] Necessariamente persona fisica, *ex* art. 4, comma 1, lett. *g* codice della privacy.

[8] C. DI COCCO, *cit.*, 126.

[9] M.G. MANGIA, *Sub* Art. 29, in *La protezione dei dati personali*, *Commentario al D.Lgs. 30 giugno 2003, n. 196 «Codice della privacy», cit.,* 658. S. FADDA, *commento all'art. 19,* in *La tutela dei dati personali. Commentario alla legge 675/1996*, a cura di E. Giannantonio, M.G. Losano, V. Zeno-Zencovich, Padova, 1997, 190.

[10] Art. 29, comma 2 codice della privacy. Cfr. Art. 17, comma 2 direttiva 95/46/CE: "il responsabile (...) deve scegliere un incaricato del trattamento che presenti garanzie sufficienti in merito alle misure di sicurezza tecnica e di organizzazione dei trattamenti da effettuare e deve assicurarsi del rispetto di tali misure". Per un commento generale, cfr. M.G. MANGIA, *Sub* Art. 29*, cit.*, 652 ss.

[11] Art. 17, comma 2 direttiva 95/46/CE e art. 26, 1° comma *Proposed Regulation.* Cfr. C. DI COCCO, *Soggetti che effettuano il trattamento*, op.cit., 129.

[12] Art. 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 12 febbraio 2010, 25. Al riguardo, dato che il rapporto controller-processor può essere inteso come un rapporto di mandato (vd. nota 13), l'ordinamento italiano è molto

D'altronde, in una decisione arbitrale riportata in un'*Opinion* dell'*Art. 29 Data Protection Working Party* (di qui in avanti Art.29WP) si è stabilito che un *provider* di un servizio di posta elettronica che lavorava per conto della Pubblica Amministrazione dovesse essere considerato "*processor*" dal momento che il suo compito, sebbene portato avanti con un certo grado di autonomia, fosse limitato soltanto ad una parte delle operazioni del trattamento di dati necessari per gli scopi determinati dal *controller*.[14]

Ciò, tuttavia, non vuol dire che il *processor* possa incidere sui tre compiti espressamente demandati al *controller* dalla normativa europea[15]: determinazione degli scopi, dei mezzi e delle misure di sicurezza riguardo al trattamento dei dati personali.

Al contrario, se il *processor* va oltre il suo mandato[16] ed acquisisce un ruolo rilevante nella determinazione degli scopi e dei mezzi diventa un *joint controller* piuttosto che un mero processor[17]. Ciò è esplicitato anche dal testo della *Proposed Regulation* all'art. 26, comma 4.

In questa chiave va letto un chiaro approccio funzionalistico alla determinazione dei ruoli, a vantaggio dell'utente, piuttosto che una lettura formalistica che porti ad un affievolirsi delle responsabilità.[18]

Ultimo dato fondamentale per ricostruire il rapporto *controller-processor* e poterlo poi calare nel contesto in esame riguarda le modalità di comunicazione delle istruzioni da parte del *controller* nei confronti del *processor*.

Le istruzioni vanno comunicate per iscritto. Ciò è esplicitato chiaramente dalla direttiva 95/46/CE, che all'art. 17 parla della necessità di un contratto o di un atto giuridicamente vincolante che regoli le relazioni tra *data controller* e *data processor*[19]. Tale contratto (o atto) deve avere forma scritta a fini probatori e deve avere un contenuto minimo che stipuli in particolare che il *data processor* agisca soltanto sotto istruzioni del *controller* e implementi misure tecniche e organizzative per proteggere adeguatamente i dati personali. Il contratto, dunque, dovrebbe includere una descrizione sufficientemente dettagliata del mandato del *processor*.[20]

Anche la *Proposed Regulation* sembra non lasciare adito a dubbi al riguardo: l'art. 26, al comma 2 riprende la suesposta disposizione della direttiva del 1995, postulando tuttavia che l'atto vincolante preveda maggiori obblighi: l'impiego di personale obbligato alla riservatezza, l'impiego di un altro *processor* solo se autorizzato, l'utilizzo di tutte le misure per il trattamento presenti nel regolamento, la

---

chiaro: l'art. 1708, 1° c., c.c., recita che "il mandato comprende non solo gli atti per i quali è stato conferito, ma anche quelli che sono necessari al loro compimento". Cfr. anche C. DI COCCO, *cit.*, 132.

13 Secondo Art. 29 Data Protection Working Party, (*ult.op.cit.*, 25) il rapporto *controller-processor* rappresenta un rapporto di mandato. Tesi che trova ampia accoglienza nella dottrina italiana: cfr. A. DEL NINNO, *La tutela dei dati personali. Vademecum sulla privacy informatica,* Ed. *Il Sole 24 ore,* 1997, 29 ss.; M.G. MANGIA, *ult.op.cit.*, 659. Si tratterebbe infatti di una normativa sovrapponibile a quella del mandato con rappresentanza *ex* art. 1704 c.c.

14 *Ibidem, example n. 17, 25*

15 Art. 2, c.1, lett. d, direttiva 95/46/CE. Nell'ordinamento italiano: art. 28 codice della privacy. Cfr. anche art. 22 *Proposed Regulation.*

16 Conformemente al dettato dell'art. 1711, 1° comma, c.c.

17 Art. 29 Data Protection Working Party, *Opinion on "controller" and "processor", cit.*, 25; cfr. anche Article 29 Data Protection Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128 (2006), p.11, in cui il *service provider* belga SWIFT è da considerarsi "controller" e non più "processor" dal momento in cui ha deciso di permettere l'accesso ai dati al Dipartimento del Tesoro degli USA senza informare gli utenti, dimostrando così di avere il potere di prendere decisioni critiche riguardo alla sicurezza dei dati, che si riverberano sugli scopi del trattamento.

18 *Ibidem,* 18.

19 Tale obbligo è ribadito all'art. 29, comma 4 del codice della privacy, ove si specifica che i compiti affidati al *processor* sono specificati "analiticamente" e "per iscritto" dal *controller*.

20 Cfr. C DI COCCO, *cit.*, 131. Tuttavia, oltre alle critiche per un sostanziale aumento di burocratizzazione nella gestione di impresa derivante da tale disposizione, per cui si veda Ri. IMPERIALI e Ro. IMPERIALI, *La tutela dei dati personali, cit.*, 80, si è comunque puntualizzato che il requisito della forma scritta non sembra richiedere necessariamente che il *processor* sia designato con un documento specificamente sottoscritto dal *controller*: in effetti qualora il rapporto non sorga con un contratto, è sufficiente un qualsiasi documento scritto riferibile al suo autore, anche se non munito della firma autografa del medesimo. In questo caso, infatti, si tratterebbe Al riguardo, M.G. MANGIA, *ult.op.cit.*, 658; V. GAGLIARDI, *sub* art. 30, *cit.*, 672; riguardo al requisito della forma per gli atti non contrattuali, cfr. C.M. BIANCA, *Diritto Civile 3*, Milano, 2000, 278 e in giurisprudenza, con specifico riguardo al contratto di mandato, Cass. n. 2306 del 1973.

collaborazione all'adempimento degli obblighi del *controller*, anche fornendo tutte le informazioni in suo possesso ed astenendosi dal trattare altrimenti i dati.[21]

III. PROBLEMI PER IL CLOUD COMPUTING

La disciplina europea appare dunque chiara riguardo ai soggetti che effettuano il trattamento dei dati personali e ai loro rispettivi compiti.

Ciò che appare invece più difficile è calare tale assetto di ruoli e qualifiche nel contesto del *cloud computing*. Lo stesso Art.29WP ha sottolineato come il *cloud computing* stia annebbiando la distinzione tra *data controller*, *data processor* e soggetto interessato.[22]

Appare doveroso innanzitutto domandarsi quali soggetti possano concretamente fungere da *controller* e quali da *processor* nel contratto di *cloud* e di conseguenza se tale assetto sia di efficace utilizzo alla luce della tecnologia emergente in esame.

1. IL *CLOUD PROVIDER* COME *CONTROLLER*: *USER-RELATED PERSONAL DATA*

Il *cloud provider* è sicuramente il soggetto la cui definizione risulta più ambigua ai fini della trattazione in esame: egli, infatti, si atteggia talora a *controller* talora a mero *processor,* a seconda del diverso quadro in cui avviene il trattamento dei dati.

Data la complessità dell'ambito, sia dal punto di vista tecnologico sia dal punto di vista normativo, occorre analizzare i diversi casi possibili di trattamento dei dati all'interno del *cloud service*: la prima ripartizione da considerare è sul tipo di dati (*user-related* o *cloud-processed*), successivamente sul tipo di *cloud* e sulla sua architettura.

Un primo livello di trattamento dei dati personali è quello che riguarda le informazioni richieste dal *cloud provider* all'utente per la realizzazione dell'*account* e dunque per la registrazione dell'utente al *cloud service*. Si tratta dei cosiddetti "*user-related personal data*".

La quantità di tali dati può variare da un livello minimo, come nel caso delle *Infrastracture as a service,* in cui si richiedono i dati minimi necessari per l'operatività di un profilo utente (nome, cognome, nazionalità, indirizzo email), ad un livello massimo, come nel caso dei profili su alcuni *Software as a Service,* ed in particolare sui *social network*.[23]

Appare chiaro che, in questo caso, chi determina gli scopi e i mezzi del trattamento è il *provider*, che dunque è indiscutibilmente un *controller*.[24]

Riguardo al trattamento di tali dati, dunque, fanno fede le *privacy policies* allegate al contratto di *cloud* e sottoscritte dall'utente al momento dell'accettazione: esse fungono, in questo contesto, da

---

[21] Cfr. i parametri cui il contratto tra *controller* e *processor*, soprattutto in relazione al *cloud computing*, dovrebbe conformarsi affinché sia efficace: Art.29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing* (WP 196), 1 luglio 2012, 14.

[22] Article 29 Data Protection Working Party and Working Party on Police and Justice, *The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168, 2009, 41.

[23] Riguardo alla rilevanza dei c.d. "*metadata*" prodotti dal *cloud provider* cfr. C. REED, '*Information "Ownership" in the Cloud*', Legal Studies Research Paper No 45/2010, Queen Mary School of Law, p. 11 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461.

[24] W.K. HON, C. MILLARD, I. WALDEN, *Who is responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Pt. 2*, Legal Studies Research Paper No. 77/2011, Queen Mary University of London, School of Law, 11.

consenso che l'interessato del trattamento dà al *controller* riguardo agli scopi, alle modalità del trattamento ed all'eventuale comunicazione di dati a soggetti terzi.[25]

2. *SOCIAL NETWORKS*: I DATI AL CONFINE TRA "*USER-RELATED*" E "*CLOUD-PROCESSED*" E LA *HOUSEHOLD EXEMPTION*

Il complicarsi delle strutture e delle funzionalità di alcuni tipi di *cloud* rende opinabili anche le considerazioni apparentemente ovvie finora svolte e la stessa bipartizione originaria tra dati di profilo (*user-related*) e dati meramente ospitati dal *provider* (*cloud-processed*).

Infatti, nei *Software as a Service* ed in particolare nei servizi di *social networking* spesso è il singolo utente a decidere quali dati inserire nel proprio profilo utente e con quale grado di visibilità nei confronti di altri utenti dello stesso servizio con un notevole grado di discrezionalità.[26]

Nonostante ciò, l'Art.29 WP dichiara[27] che i *social network provider* devono essere considerati "*data controller*" ai sensi della direttiva sulla protezione dei dati, mentre i terzi soggetti che eventualmente sviluppano programmi o applicazioni ulteriori su quel *social network* "possono" essere considerati *data controller* se l'utente sceglie di usare le dette applicazioni.[28] Gli utenti, infine, sono da considerarsi meri soggetti del trattamento (o "interessati", ai sensi della definizione fornita dall'art. 4, lett. *i*, del nostro Codice dei dati personali) e, qualora si dimostrasse che agiscano da *controller,* essi sarebbero comunque coperti dalla c.d. *household exemption* ai sensi dell'art. 3, comma 2 della direttiva 95/46/CE (e l'art. 2, comma 2, lett. D della *Proposed Regulation*).[29]

Tuttavia, come riconosce la già citata *Opinion* dell'Art.29WP, la *household exemption* non può esonerare dalla disciplina gli utenti che agiscano per conto di compagnie od associazioni (poiché mancherebbe *de facto* il requisito della "persona fisica" di cui all'art. 3, comma 2) o utilizzino la piattaforma principalmente per finalità commerciali, politiche o sociali diffuse (poiché mancherebbe il requisito dell'uso domestico o personale dei dati). Inoltre, qualora i contatti auto-selezionati con cui è in relazione l'utente siano numericamente elevati (con la conseguenza che molti contatti-utenti siano potenzialmente sconosciuti all'utente che tratta i dati), o se l'utente, nell'ambito della discrezionalità

---

[25] Riguardo alla comunicazione a soggetti terzi di certi dati, per esempio, Dropbox.com assicura di "non vendere informazioni personali a terze parti", ma al massimo condividerle con aziende che in *outsourcing* sono deputate ad implementare un particolare servizio (https://www.dropbox.com/privacy), al contrario le *privacy policies* della Apple (http://www.apple.com/privacy/) non escludono esplicitamente la vendita di dati personali a terzi ed anzi parlano di "cessione" a soggetti terzi che il *cloud provider* ritiene "partner commerciali rilevanti".
Infine Facebook afferma di "fornire dati agli inserzionisti partner o clienti solo dopo" aver proceduto ad opportuna anonimizzazione dei dati (https://www.facebook.com/full_data_use_policy), conformemente a quanto indicato dal considerando n. 26 della direttiva 95/46/CE.

[26] Cfr. per esempio Normativa sull'utilizzo dei dati di Facebook, Sez. II "Condivisione e possibilitàà di trovarti su Facebook" (ultima revisione 11 dicembre 2012), https://www.facebook.com/full_data_use_policy.

Riguardo ai risvolti giuridici della "nuova" autonomia strutturale dell'utente nel web 2.0 cfr. M. PEGUERA, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems,* Col.Jour. Law&Arts, 32:4, 2009, 481 ss. In particolare si rilevano due sentenze francesi *(Flach Film v. Google France*, *Google Inc.*, Tribunal de commerce, Paris 8e ch., Feb. 20, 2008 e *Zadig Productions v. Google Inc.*, Afa, Tribunal de grande instance, Paris, 3e ch., 2e sec., Oct. 19, 2007) in cui non si ritiene sufficiente, per considerare "*publisher*" (e dunque responsabile) il gestore del sito, il mero fatto di aver determinato l'architettura e il layout del sito, ma ciò che rileva è piuttosto l'autonomia concessa agli utenti nel generare e rendere pubblici i contenuti.

[27] Art. 29 Data Protetcion Working party, *Opinion 5/2009 on online social networking*, adottata il 12 giugno 2012, p. 12.

[28] *Ibidem, 5*.

[29] La *household exempion* (o *exception*) prevede che le "persone fisiche" che effettuino dei trattamenti "senza finalitàà di lucro per l'esercizio di attivitàà esclusivamente personali o domestiche" non siano sottoposte ai vincoli e agli obblighi della disciplina europea sul trattamento dei dati personali. Per una ricognizione sulla normativa italiana in merito, cfr. M. GORGONI, *Commento all'art. 5, 3° comma*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati poersonali, Commentario al D.lgs. 30 giugno 2003, n. 196*, Tomo I, Padova, 2007, 97-123.

summenzionata, decide addirittura di rendere visibile a tutto il web certi dati, non può applicarsi l'eccezione in esame poiché mancherebbe il requisito dell'uso "domestico".[30]

D'altronde, anche la Corte di Giustizia Europea[31] si è espressa più volte sulla *household exception* chiarendo che essa deve interpretarsi nel senso di comprendere unicamente le attività che rientrano nell'ambito della vita privata o familiare dei singoli e che qualora il trattamento comporti la trasmissione dei dati ad un numero indefinito di persone (come la pubblicazione su un profilo accessibile a tutti) l'eccezione non può sussistere, come confermato anche dal Garante Europeo sulla Protezione dei dati.[32]

Pertanto, in tutti questi casi l'utente è a tutti gli effetti un *data controller*, che comunica dati personali ad altri *controller* (come il *Social network provider*) e a terze parti (ovvero gli altri utenti del servizio), con tutti gli obblighi derivanti dalla disciplina europea e dalle leggi nazionali.

Comunque, non si può non sottolineare un'importante specificazione posta dalla *Proposed Regulation*: il considerando n. 15, infatti, chiarisce che la esenzione in oggetto non riguarda *controllers* o *processors* che forniscono i mezzi per il trattamento di dati per attività domestiche o personali. Posto dunque che il *controller* sia l'utente, si viene così a creare una situazione paradossale per cui il *processor* è sottoposto ai vincoli della direttiva, mentre il *controller* (che per definizione è il responsabile primario) gode di un'esenzione piena riguardo al trattamento.

Inoltre, si è fatto notare che anche al di fuori della *household exemption*, l'utente può beneficiare di altre "esenzioni" dettate dai principi generali dell'ordinamento: come la libertà di espressione (artistica, letteraria, giornalistica), come chiarito dall'art. 9 della direttiva 95/46/CE e dall'art. 80, comma 1 della *Proposed Regulation*.[33]

Occorre, inoltre, menzionare la proposta emersa in dottrina di rendere l'esenzione meno rigida e più limitata, in modo da evitare vuoti di protezione per alcuni trattamenti di dati nel pericoloso mondo delle infrastrutture *cloud*.[34]

Comunque, la *household exemption* non esonera dall'eventuale responsabilità penale e civile che un danno a terzi comporterebbe ai sensi delle discipline nazionali.[35]

---

[30] Art. 29 WP, *Opinion 5/2009 on online social networking*, adottata il 12 giugno 2012, 6.

[31] Sent. CGE, 12 settembre 2007, causa C-73/07, Satamedia, Racc. pag. I-9831, punto 47 che riprende la Sentenza CGE, 6 novembre 2003, causa C-101/01, Lindqvist, Racc. pag. I-12971, punti 43 e 44.

[32] European Data Protection Supervisor (P. HUSTINX), *Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*, 16 novembre 2012, par. 41.

[33] *Ibidem*: appare chiara una necessitàà di bilanciamento tra i diritti in questione. Riguardo al rapporto tra libertàà di espressione e diritto alla privacy cfr. Sent. CGE, *Lindqvist*, *cit*., parr. 30, 73-78 e conclusione n. 5.

Nell'ambito del bilanciamento tra diritto alla protezione dei dati (art. 8 Carta di Nizza) e altri diritti fondamentali occorre menzionare anche altri importanti interventi della giurisprudenza comunitaria: cfr. Sent. CGE Caso *Sabam* v. *Scarlet Extended* (C-70/10), parr. 50-52; Caso *Sabam v. Netlog* (C-360/10), parr. 49-51, in cui il "diritto alla privacy" (insieme al diritto alla libertàà di impresa *ex* art. 16 Carta di Nizza e alla libertàà di informazione *ex* art. 11) si pone in contrasto con l'esercizio del diritto alla proprietàà intellettuale (art. 17, n. 2 Carta di Nizza), al punto che vengono impedite agli *internet service provider* attivitàà di "filtraggio controverso" generalizzato sul materiale inserito nei *server* dagli utenti, anche perché ciò "implicherebbe l'identificazione, l'analisi sistematica e l'elaborazione delle informazioni relative ai profili creati sulla rete sociale dagli utenti della medesima - o gli indirizzi IP per i meri "fornitori di accesso ad Internet"-, informazioni, queste, che costituiscono dati personali protetti, in quanto consentono, in linea di principio, di identificare i suddetti utenti". (Caso *Netlog*, par. 49; Caso *Scarlet*, par. 51).

[34] Y. POULLET, J.-M. VAN GYSEGHEM, J. GÉRARD, *et al.* (Research Centre on IT and Law (CRID)), *Discussion paper 'Cloud computing and its implications on data protection'* (Council of Europe, 2010), 12. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf

[35] M. GORGONI, cit., 101; Cfr. anche E. NAVARRETTA, Commento sub art. 9, in *Tutela della Privacy. Commentario alla L. 31 dicembre 1996, n. 675*, a cura di C.M. Bianca e F.D. Busnelli, in *Le Nuove leggi civile commentate*, Padova, 1999, n. 2-3, 325-326. È bene notare che la legge precedente (n. 675/1996) prevedeva all'art. 3, comma 2 che la *household exemption* non riguardasse anche la responsabilità civile (art. 18, oggi art. 15 codice della privacy), penale (art. 36, oggi art. 169 codice della privacy), a cui erano dunque sottoposti anche coloro che facevano mero uso personale di tali dati. Cfr. G. CORASANTI, *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali*, in R. PARDOLESI, (a cura di), *Diritto alla riservatezza e circolazione dei dati personali,* Milano, 2003, vol.II, pp. 546, ss. Tuttavia, in seguito al d.lgs. 467/2001 e alle modifiche della disciplina apportate dallo stesso codice del 2003, tale riferimento è stato eliminato. Ciononostante, in dottrina si è discusso se da ciò derivasse automatica esclusione di qualsiasi forma di responsabilità civile e penale per colui che fa un uso personale dei dati. Se ciò può apparire pacifico, anche per esigenze di legalità delle norme penali, cfr. S. DEL CORSO, Commento sub artt. 34-38, in *Tutela della Privacy*, *cit*., 735, il riferimento a "chiunque" (degli artt. 15 e 169) conserva la responsabilità penale e civile per l'omessa adozione delle misure di sicurezza (*ex* art. 33) anche per chi fa uso personale dei dati, poiché tali

D'altro canto, ci sono diverse informazioni che l'utente non fornisce spontaneamente al *social network provider*, ma che quest'ultimo ricava da terzi e che spesso comunica agli altri utenti. Si tratta di geolocalizzazione, cronologia degli URL consultati, indirizzo IP, o più in generale gusti personali o preferenze commerciali dell'utente comunicati da terzi partner inserzionisti, gradimenti manifestati sul *social network* (i c.d. *likes*), tramite la partecipazione dell'utente ad applicazioni o giochi collegati al *social network,* ma anche data e ora in cui si è acceduti all'applicazione, o di informazioni fornite da altri utenti (come fotografie o informazioni personali).[36]

Se tutto ciò è contemplato dalle *privacy policies* è chiaramente lecito ed in questo caso è indubbio che l'unico *controller* sia il *cloud provider.*[37]

Occorre tuttavia rilevare che molti dati trattati dal *social network* rientrano nella sfera dei dati sensibili.[38] Per esempio i succitati "*likes*" sono, in quanto espressione di gradimento, atti a rilevare "le opinioni politiche, le convinzioni religiose o filosofiche" e "la vita sessuale".[39] Addirittura le foto caricate su un *social network* potrebbero essere una categoria speciale di dati sensibili atti a rivelare origine etnica, credenze religiose o stato di salute. Tuttavia l'Art.29WP si rifiuta di identificare automaticamente le foto tra i dati sensibili.[40]

Per tali dati, dunque, occorre un consenso esplicito dell'utente al trattamento e alla diffusione, che prescinde dalla mera comunicazione spontanea al *provider* di tali dati o dalla mera sottoscrizione delle *privacy policies* al momento dell'iscrizione al servizio.[41]

Qualora si dimostri che per quel particolare trattamento di dati il *controller* non sia il *provider,* ma l'utente stesso o un utente terzo, il consenso esplicito va richiesto dall'utente.

Da quanto finora detto, appare chiaro che la definizione del ruolo dell'utente e di quello del *provider* ai fini del trattamento dei dati è un problema irrisolto alla luce della direttiva 95/46/CE.

Tuttavia, la disciplina sembra cambiare con la *Proposed Regulation*, ove viene regolata esplicitamente la figura intermedia del *joint controller* o corresponsabile del trattamento[42], in cui la qualifica del *controller* si configura come ruolo partecipato e potenzialmente pluripersonale.[43]

3. *CLOUD PROVIDER* TRA *CONTROLLER* E *PROCESSOR*: I *CLOUD-PROCESSED PERSONAL DATA*

Di più problematica definizione, invece, è il caso in cui l'utente utilizzi il *cloud* per inserirvi e conservarvi dati di propria spontanea scelta: non si tratta più di *user-related personal data* (vd. *supra*), ma di *cloud-processed personal data.*[44]

Questo è il caso, ad esempio, del normale uso di un *cloud service* come contenitore di *file,* situazione peraltro simile alla già affrontata condivisione spontanea di dati su un *social network* (*post*, commenti,

misure costituiscono una soglia minima propria anche del trattamento di dati per fini personali. Cfr. R. CLARIZIA, *Legge 675/1996 e responsabilità civile,* in *Diritto dell'Informazione*, 1998, 245; M. GORGONI, *cit*., 125; sul valore del riferimento al "chiunque", cfr. anche G. BUTTARELLI, *Banche dati e tutela della riservatezza,* cit., 351; D. CARUSI, *La responsabilità,* in *La disciplina del trattamento dei dati personali,* a cura di V. Cuffaro e V. Ricciuto, Torino, 1998, 377.

[36] Cfr. Normativa sull'utilizzo dei dati di Facebook, Sez. I. "Informazioni ricevute da Facebook e relative modalità di utilizzo" https://www.facebook.com/full_data_use_policy.

[37] Cfr. Il caso dell'introduzione dei "*like*" di *Facebook* sul sito web del servizio sanitario del Regno Unito, che permetteva a *Facebook* di controllare quali pagine su quel sito erano visitate dagli utenti di *Facebook*, '*NHS.uk allowing Google, Facebook, and others to track you*' (Garlik blog, 23 November 2010), http://www.garlik.com/blog/?p=405. Cfr. W.K. HON, *ult.op.cit*., nota 93.

[38] Ai sensi dell'art. 8, comma 1 della direttiva 95/46/CE.

[39] Come dalla lettera dell'art. 8, comma 1 della direttiva 95/46/CE

[40] Art. 29 Data Protetcion Working party, *Opinion 5/2009 on online social networking*, adottata il 12 giugno 2012, 8.

[41] *Ibidem.*

[42] Art. 24, *Proposed Regulation.*

[43] vd. par. 5

[44] W.K. HON *et al.*, *ult.op.cit.*, 11.

foto, *status*), con la differenza che questi ultimi sono al limite tra "*user-related*" e "*cloud-processed*" e perciò particolarmente problematici[45].

Per definire chi sia il *controller* di tale trattamento occorre chiarire chi definisce gli scopi dello stesso, oltre che i mezzi (ai sensi dell'art. 2, lett. D della direttiva del 1995), le condizioni (dell'art. 4, n.5 della *Proposed Regulation*), il profilo della sicurezza (art. 4, comma 1, lett. F del codice della privacy) e chi invece esegue meramente istruzioni altrui.

Affinché tale operazione risulti corretta, però, è necessario separare le ipotesi in cui il trattamento di dati avviene su un *cloud* del tipo *IaaS* da quelle in cui il trattamento è effettuato su un *cloud* del tipo *SaaS*.[46]

Nel primo caso, colui che determina le finalità, gli scopi è sicuramente l'utente: egli soltanto conosce i motivi per cui archivia, cataloga, conserva alcuni dati personali (suoi e/o altrui).[47]

Colui che determina i mezzi, inoltre, è (almeno in larga parte) l'utente: egli, infatti, è libero di catalogare i dati nel modo che ritiene più adatto e attraverso fogli di calcolo o tipi di formato che preferisce, senza che il "contenitore" *cloud* incida su tale scelta (salvo per il limite di memoria di cui l'infrastruttura dispone).[48]

Da tale ricognizione superficiale potremmo concludere che il *cloud client* in questo caso è un *controller* del trattamento dei dati, conformemente a quanto stabilito dall'Art.29 WP[49]. Dunque l'utente sarebbe il principale soggetto responsabile per la protezione e la sicurezza dei dati.[50]

Tuttavia, vanno rilevate due questioni che possono rendere più complessa tale conclusione.

Innanzitutto, è bene ricordare la già menzionata "*household exemption*" (all'art. 3, comma 2 della direttiva del 1995 e all'art. 2, comma 2, lett. D della *Proposed Regulation*, vd. *supra*) e i casi, dunque, in cui il trattamento non rientra nell'ambito di protezione della disciplina europea, consci tuttavia che il *provider* per la *Proposed Regulation* è comunque sempre vincolato[51] dalla disciplina europea, salvo si opti per definirlo né un *controller,* né un *processor*, come si discuterà in seguito.[52]

In secondo luogo, occorre una più attenta valutazione in concreto del ruolo dell'utente (e del *provider*) nel contesto in esame e della sua rispondenza alla qualifica di *controller*.

Come infatti rileva il Garante Europeo, la complessità dei mezzi tecnologici impiegati nell'ambiente *cloud*, ha raggiunto un tale livello che è necessario chiarire che il *controller*/utente può non essere la sola entità che determina scopi e mezzi,[53] pur risultando tuttavia il responsabile primario a livello penale e civile: è chiaro lo sbilanciamento dell'assetto dei rapporti a svantaggio del *controller*.

Va tuttavia rilevato che, nella fase di discussione della *Proposed Regulation*, diversi emendamenti[54] sono tesi a rimuovere la determinazione di "mezzi e condizioni" tra i requisiti per la definizione del *controller*. Egli rimarrebbe così il mero definitore degli scopi del trattamento, dunque non ci sarebbe più nessun ostacolo nel considerare l'utente come unico *controller* (dei *cloud-processed data*). Tuttavia, tale proposta ha per ora ricevuto parere contrario da parte del Garante europeo per la Protezione dei Dati.[55]

Comunque, stando così le cose, il soggetto che nel contesto in esame determina effettivamente scopi, mezzi e condizioni non sembra essere di facile identificazione.

---

[45] vd par. 3.3.

[46] Per i *cloud* di tipo *PaaS*, invece, trattandosi di una posizione intermedia agli altri due tipi, occorre una valutazione concreta delle funzioni che il *provider* assume ai fini del servizio.

[47] W.K. HON *et al.*, *op.ult.cit.*, 22.

[48] Art. 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor", cit.,* 28.

[49] *Ibidem.*

[50] D. CATTEDDU, G. HOGBEN, *Cloud Computing - Benefits, risks and recommendations for information security* (European Network and information Security Agency, 2009), 66.

[51] Considerando n. 15, *Proposed Regulation,* che afferma che i *controller* e i *processor* di un trattamento coperto dalla *household exemption,* sono comunque vincolati agli obblighi della testo di legge in esame.

[52] vd. par.

[53] European Data Protection Supervisor (P. HUSTINX), *Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*, 16 novembre 2012, par. 52.

[54] ITRE AM 81; IMCO AM 62; LIBE AM 746, 747, 748.

[55] European Data Protection Supervisor, *Additional Comments on the Data Protection Reform Package*, Brussels, 15 marzo 2013, par. 24.

L'utente, infatti, ha il potere di rendere visibili i suoi dati solo a determinati soggetti, semmai di utilizzare linguaggi criptati e comunque ha il dovere di usare diligentemente i dati a sua disposizione.[56] Tuttavia, la sua autonomia risulta limitata dal *cloud provider* per una serie di ragioni esposte qui di seguito. In primo luogo il *provider* tipicamente progetta, aggiorna e manutiene l'infrastruttura *cloud* in piena autonomia.[57]

Inoltre, nella maggior parte dei casi l'utente non conosce la reale allocazione dei *server* del *cloud* e dunque non conosce la posizione effettiva dei dati e la legge conseguentemente applicabile.[58] Tale ultimo problema, tuttavia, sarà in parte risolto dai forti vincoli posti in materia di "trasferimento di dati personali verso paesi terzi o organizzazioni internazionali" dalla *Proposed Regulation*. Infatti, è esplicitato che le regole sul trasferimento dei dati vanno applicate anche ai *processor*[59], rendendo inutile lo sforzo di definizione dei ruoli in questo ambito, e sono richieste precise garanzie contrattuali da rispettare.[60] Tuttavia, perplessità restano anche con l'attuale proposta di regolamento, al punto che è stato suggerito, in sede di discussione, un nuovo articolo (44a) che regoli specificamente il trasferimento di dati a servizi *cloud* che operino sotto la giurisdizione di paesi terzi, prevedendo obblighi precisi in cambio di trasparenza.[61]

Al momento, tuttavia, la soluzione del problema in questione è affidata alle previsioni contrattuali del servizio, posto che il cliente non può mai accettare termini contrattuali in violazione della disciplina europea.[62]

Comunque, in quanto mero "consumatore"[63] di un servizio di *cloud*, egli non è informato su eventuali spostamenti di dati da un server all'altro del *provider*[64] o sul possibile trasferimento della gestione informatica dei suoi dati in *outsourcing* ad aziende terze, se non per meri richiami generici nel proprio contratto di *cloud*.[65]

Inoltre, l'utente non conosce le persone fisiche che effettueranno concretamente il trattamento: la sua unica interfaccia è il *cloud provider*, a cui è legato da un contratto elettronico standard, che non può far altro che accettare o rifiutare *in toto*, senza la minima negoziazione possibile.[66]

Non si trascuri, infatti, che il *cloud service* si basa su un contratto - tendenzialmente un formulario *standard* - che obbliga un *cloud provider* a fornire all'utente un servizio di *mass storage* (ma anche fogli di calcolo, ecc.) *online*.

---

[56] *Ibidem*, par. 41.

[57] *Ibidem*, par. 52.

[58] Y. POULLET, J.-M. VAN GYSEGHEM, J. GÉRARD, *et al*., *cit*., 11.

[59] Art. 40. Cfr. EDPS, *Opinion on the Data Protection Reform Packag*e, *cit*., par. 214.

[60] Art. 42. Cfr. EDPS, *Opinion on the Data Protection Reform Packag*e, *cit*., 221-223.

[61] Emendamento LIBE AM 2531, Cfr. European Data Protection Supervisor, *Additional Comments on the Data Protection Reform Package, cit.,* par. 39 che si dichiara contraria a tale emendamento, poiché specificando una particolare tecnologia rispetto ad altre rischia di non essere tecnologicamente neutrale.

[62] Art. 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor", cit.,* 26 e Art. 29 Data Protection Working Party, *Opinion 5/2012, cit*., 14. Per un quadro generale sull'argomento si rimanda a W. K. HON, J. HORNLE, C. MILLARD, *Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3,* Queen Mary University of London, School of Law Legal Studies Research Paper No 84/2011.

[63] Sulla definizione del *cloud user* come "consumatore", con tutti i dubbi per gli utenti che agiscano non come privati, ma per conto di aziende o nello svolgimento di una professione cfr. A. CUNNINGHAM, *Caveat Consumer? – Consumer Protection and Cloud Computing - Pt. 1*, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 130/2013.

[64] Cfr. D. CATTEDDU, G. HOGBEN, *cit*., 67-68.

[65] Cfr. per esempio la *Privacy policy* della *Apple* (http://www.apple.com/privacy/) in cui si fanno richiami generici a possibili terzi soggetti: "*At times Apple may make certain personal information available to strategic partners that work with Apple to provide products and services, or that help Apple market to customers*". Diverso, invece, il caso di Dropbox, che non prevede ipotesi di *outsourcing,* ma specifica che per eventuali fusioni o scissioni aziendali le informazioni possono essere trasferite a terzi, ma solo in seguito a notifica all'utente, una notifica che riguarda anche qualsiasi cambio nel controllo o uso di informazioni personali (https://www.dropbox.com/terms). In merito al problema dell'allocazione geografica internazionale degli operatori della società dell'informazione, cfr. lo storico caso *LICRA v. Yahoo*, *Tribunal de Grande Instance de Paris,* 20-11-2000*,* in *Electronic Business Law Reports,* 1(3), 2001*,* 110 ss.*,* con nota di Y. HAKDENIZ.

[66] A. CUNNINGHAM, *Caveat Consumer? – Consumer Protection and Cloud Computing - Pt. 2*, Queen Mary University of London, School of Law, Legal Studies Research Paper No. 133/2013, 3. Per un approfondimento sul tema cfr. anche S. BRADSHAW, C. MILLARD e I.WALDEN, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper No. 63/2010. http://ssrn.com/abstract=1662374.

Nei casi in cui l'utente sia definito *controller* e il *cloud provider* sia quindi *processor* del trattamento, occorre rilevare che il contratto di *cloud service*, a prescindere dal concreto tipo contrattuale a cui è ravvicinato, ai fini della normativa sulla *privacy* si atteggia a contratto di mandato ed è dunque quel documento scritto indicato come necessario ai sensi dell'art. 17 della direttiva 95/43/CE ed anche dell'approvando regolamento (art. 26, comma 2).[67]

Sorge spontaneo il dubbio che un mero formulario standard predisposto dal *processor* non possa costituire un valido strumento con cui il *controller* liberamente istruisca e delimiti l'operato del *processor*, obbligandolo a precise prestazioni.[68]

Chiaro è che l'asimmetria negoziale tra utente e *provider* non deve mai essere considerata una giustificazione per il *client* ad accettare termini contrattuali che siano in violazione della disciplina europea.[69]

Comunque, si ritiene che le istruzioni al *processor* debbano essere modificabili in qualunque momento, che i poteri affidati al *controller* possano essere ridotti o aumentati nel corso del trattamento, che il *controller* debba svolgere verifiche periodiche e continuate dell'operato del *processor*.[70]

In generale, l'utente-*controller* dovrebbe essere in grado di implementare appropriate misure tecnico-organizzative che assicurino che il trattamento dei dati adempia alla disciplina europea.[71]

Tutto ciò appare quasi impossibile nell'attuale assetto del *cloud* se sposiamo la dicotomia *utente-controller* e *provider-processor,*[72] con la conseguenza che è davvero molto difficile per l'utente riuscire a rispettare tutti i suoi obblighi (ai sensi della disciplina europea) senza un reale potere sul *processor*.[73]

Del resto, la *Proposed Regulation* ha inserito anche le "condizioni" tra gli elementi essenziali, ponendo così maggiore enfasi sulla responsabilità di coloro che determinano come il trattamento dei dati sia concretamente organizzato (in questo caso il *provider* che detta l'organizzazione interna della struttura di *cloud*).[74]

Caso diverso, invece, è il trattamento dei *cloud-processed data* - da parte dell'utente - all'interno di un sistema di *Software as a Service* (che sia *facebook*, oppure un foglio di calcolo *online*, ecc.).

In questo caso, la determinazione degli scopi resta in capo all'utente, poiché il *cloud provider* non influenza certo le finalità per cui un trattamento di tale tipo è posto in essere.

Tuttavia, oltre al problema della decisione delle misure di sicurezza, in questo caso neppure le "modalità del trattamento" sono determinate dall'utente.[75]

In effetti, il *cloud client* ha spazi di autonomia piuttosto limitati nei *Software as a Service* sulla determinazione delle modalità di trattamento dei dati: egli dovrà necessariamente attenersi alle possibilità infrastrutturali offerte dal *software* che sta utilizzando.[76]

Per il *Paas*, cioè per una piattaforma di software in un'infrastruttura di *cloud*, tuttavia tale spazio di autonomia - seppur costretto - è meno limitato rispetto al caso precedente: già la possibilità di scegliere uno tra più *software* a disposizione è sintomo di maggiore discrezionalità nella scelte delle "modalità" di gestione dei dati.

---

[67] Vd. par. 2.

[68] A. CUNNIGHAM, *cit.*, 32; cfr. anche G. BUTTARELLI, *Security and privacy regulatory challenges in the Cloud (Speaking notes),*The 2012 European Cloud Computing, Making the Transition from Cloud-Friendly to Cloud-Active Brussels, 21st March 2012, 2; cfr. anche Art. 29 Data Protection Working Party, *Opinion 5/2012, cit.,* 8.

[69] Vd. nota 57.

[70] C. DI COCCO, *cit.*, 132.

[71] art. 17 Direttiva 95/46/CE; art. 23 ("*data protection by design*") *Proposed Regulation.*

[72] Ciò può non solo condurre a suggerire che il *provider* sia in fondo anche *controller,* ma anche che lo stesso possa sfuggire addirittura anche dal ruolo di *processor*, come spiegato in seguito (vd. paragrafo 3.6).

[73] European Data Protection Supervisor (P. HUSTINX), *Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*, 16 novembre 2012, par. 53.

[74] *Ibidem,* par. 54.

[75] European Data Protection Supervisor (P. HUSTINX), *Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*, 16 novembre 2012, par. 57.

[76] D. CATTEDDU, G. HOGBEN, *Cloud Computing - Benefits, risks and recommendations for information security* (European Network and information Security Agency, 2009), 66.

Tuttavia, le difficoltà di identificazione dell'utente nella qualifica di *controller* nei casi suesposti non devono portare alla conclusione che il *cloud provider* sia sempre e comunque *controller* e *processor* del trattamento dei dati su *cloud*. Sarebbe un enorme onere - oltre che contrario alla lettera della legge - per i *provider* dover rispondere anche del trattamento di dati le cui finalità (e i cui mezzi almeno in parte) sfuggono alla loro volontà.[77]

Si tenga inoltre presente il caso particolare in cui l'utente è costituito da una persona giuridica.

In questa circostanza è bene sottolineare che, ai sensi dell'art. 4 della *Proposed Regulation*, non può essere "soggetto" interessato dal trattamento una persona giuridica, pertanto, quandanche si accertasse che il *provider* svolga funzioni di *controller* egli non può che essere *co-controller* insieme all'utente-persona giuridica, non potendo quest'ultimo svolgere funzione diversa.[78]

L'art.29 WP tuttavia suggerisce dei criteri che possano aiutare a qualificare i soggetti in gioco in base al concreto ruolo svolto dalle parti:[79]

il livello di istruzioni preventive fornite dal *controller*, cioè il margine di manovra lasciato al *data processor*;

il monitoraggio che il *data controller* ha dell'esecuzione del servizio. Una costante e attenta supervisione svolta dal *controller* sull'adempimento del *processor* alle istruzioni fornite (e ai termini del contratto) è indice che il *controller* è ancora nel pieno ed esclusivo controllo del trattamento;

visibilità/immagine data dal *controller* al soggetto interessato del trattamento e le conseguenti aspettative del soggetto riguardo all'esercizio dei suoi diritti;

perizia delle parti (talvolta il ruolo tradizionale e la perizia professionale del *provider* può far di lui un *controller*).

Da quanto sopra detto, appare però chiaro che alla luce di questi quattro punti l'utente non svolge una piena funzione di *controller*, al contrario sembra che quanto a perizia, visibilità, potere negoziale, e (mancanza di) possibilità di controllo da parte dell'utente, sia il *provider* a detenere molte delle funzioni che svolge un *controller*.

4. Analisi dei singoli Terms of Use: alla ricerca della qualifica del cloud provider e dell'utente

Per esaminare meglio il concreto rapporto tra le parti alla luce dell'elenco sopra riportato, può risultare interessante un'analisi dei *Terms of Use* (contratto, ma anche *privacy policy)* dei diversi *cloud service*, pur consci che i termini contrattuali che cercano di definire lo *status* del *provider*, come *controller* o *processor*, non sono determinanti ai fini della disciplina europea.[80] Sono infatti le circostanze concrete che determinano la reale configurazione dei ruoli, anche se ovviamente i termini contrattuali possono influire su tale configurazione, in quanto regolamento del rapporto tra soggetti coinvolti nel trattamento.[81]

Riguardo agli *user-related data* il problema non si pone: come si è già sopra spiegato tale identificazione è pressoché pacifica, del resto molti *provider* si definiscono autonomamente *controller* di tali dati.[82]

---

[77] W.K. HON, *et al., ult.op.cit.,* 18.

[78] Cfr. European Data Protection Supervisor (P. HUSTINX), *Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*, 16 novembre 2012, par. 47.

[79] Art. 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor", cit.,* 29.

[80] Cfr. Article 29 Data Protection Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128 (2006).

[81] W.K. HON, *ult.op.cit.*, 14.

[82] W.K. HON, *ult.op.cit.*, 12.

Riguardo, invece, al trattamento dei *cloud-processed data* la maggior parte dei fornitori di servizi *cloud* non fa esplicito riferimento alla propria qualifica al riguardo.[83]

Alcuni semplicemente non si esprimono[84], altri invece riconoscono che i propri utenti possano trattare dati personali, forse anche di soggetti terzi, all'interno dei documenti che essi liberamente affidano al servizio di *storage*. Tuttavia, il *provider* si definisce "contenitore passivo" di tali dati (definiti "*hosted data*" a simboleggiare la sua estraneità dagli stessi) che non svolge una concreta attività di raccolta e spesso non accede neppure a tali dati (salvo per fornire supporto ai clienti o implementare alcuni servizi),[85] sulla stessa scia anche altre aziende che si definiscono intermediari o meri agenti.[86]

Altri, invece, più esplicitamente dichiarano che l'utente è un *controller* per il trattamento di quei dati[87] (anche attraverso riferimenti impliciti)[88] o che è responsabile a rimborsare il provider in caso di *data breaches*[89] oppure descrivono il contenuto delle obbligazioni dell'utente, ricalcando precisamente le obbligazioni del *controller* (affermando specularmente che il provider svolge una funzione di "processing").[90] Alcuni *provider*, invece, fanno esplicito riferimento al loro *status* di *processor*.[91] Altri, invece, incorporano espressamente le clausole contrattuali standard della Commissione Europea che legittimano, nell'ambito della protezione dei dati, l'esportazione dei dati dai clienti europei al *provider* in quanto *processor*.[92]

Infine, alcuni provider di tipo IaaS mantengono una posizione neutrale, prevedendo esplicitamente situazioni in cui il *provider* sia *controller* e altre in cui esso sia *processor*,[93] ed accennando così

---

[83] S. BRADSHAW, C. MILLARD and I. WALDEN, '*Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*', Queen Mary School of Law, Legal Studies Research Paper No 63/2010 ('CLP Contracts Paper') <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374>.

[84] *Ex multis,* cfr. *Iron Mountain Web Site Privacy Policy* (http://www.ironmountain.com/Utility/Legal/~/link.aspx?_id=6832C036B92D477CA7B90844E0B77C64&_z=z).

[85] *Ex multis,* cfr. La *Privacy policy* di *GoGrid* (un *cloud* di tipo IaaS), par. "*Hosted Data*", http://www.gogrid.com/legal/privacy-policy.php.

[86] *Akamai*, *Privacy Statement*, par. 3.: "*Akamai's processing of data is determined by our business customers. When processing data on behalf of business customers as an intermediary service provider, Akamai does not collect, use, or disclose personally identifiable consumer information, except as directed by Akamai's business customers...*" (http://www.akamai.com/html/policies/privacy_statement.html). Akamai, che copia i siti web dei suoi clienti sulla sua infrastruttura per implementare l'accessibilità di questi siti, è un ottimo esempio di un *cloud* con funzione relativamente "passiva", difficile da classificare come IaaS, SaaS o PaaS. Cfr. anche, similmente, nota 48.

[87] '*With regard to data protection laws, you are the data controller for all data stored in your account or transmitted by your virtual servers.*' ElasticHosts (IaaS), Terms of Service <http://www.elastichosts.com/cloud-hosting/terms-of-service>.

[88] Cfr. Dropbox (https://www.dropbox.com/terms), che considera il cliente "soltanto responsabile per la sua condotta, per il contenuto dei *file* e delle cartelle e le sue comunicazioni con terzi attraverso il servizio di *cloud*", prefigurando così che l'utente sia "soltanto" *controller* di tutti i dati che non siano meramente *user-related.*

[89] La "GoGrid's standard indemnity provision" alla sezione 9 richiede che i suoi utenti risarciscano il *provider* in caso di "(b) *security breaches or other alleged faults in the Service, including without limitation faults listed in the SLA and faults leading to the release or exposure of personally identifiable information or other private data (whether such data belongs to Customer, to one of Customer's customers, or to other third parties);...*" (http://www.gogrid.com/legal/terms-service.php).

[90] Microsoft, Terms of Use (The Database Manager for SQL Azure) Sez. 8 '*Your Privacy Practices*' (http://msdn.microsoft.com/en-us/library/gg442310.aspx): "*If you collect, store, or otherwise process personal information using Database Manager, you must: (a) comply with all applicable privacy and data protection laws; and (b) obtain sufficient authorization from the persons providing the information to permit the processing of the information by Microsoft, its affiliates, subsidiaries, and service providers (collectively "Microsoft Parties") as contemplated by this agreement, including (i) transfer of the information to the Microsoft Parties for their processing; and (ii) processing of the information outside the jurisdiction in which the information is provided to you, such as storage and other processing in the United States*".

[91] Cfr. W.K. HON, *et al.*, *ult.op.cit.*, p. 13.

[92] Riferendosi alla decisione della Commissione Europea 2002/16/CE del 27 Dicembre 2001 sulle clausole standard per il trasferimento di dati personali a *processor* stabiliti in paesi terzi, ai sensi della direttiva 95/46/CE, come modificato in base alla Decisione della Commissione Europea del 5 febbraio 2010 (2010/87/EU). Cfr. W.K. HON, *et al.*, *cit*, p.13.

[93] Rackspace General Terms (http://www.rackspace.co.za/legal/general-terms/), par.19: "*Each of us agrees to comply with our respective obligations under the Data Protection Act 1998 (the "Act") as applicable to personal data that it controls or processes as part of, or in connection with, its use or provision of the Services... We agree that we will not provide access to personal data that you store on your Hosted System to any subcontractor or affiliate outside of the EEA unless that person meets the requirements stated below during the entire time that it has access to the personal data: 19.1.1 for personal data for which we are a "controller" under the Act... 19.1.2 for personal data for which we are a "processor" under the Act....*" Si sottolinea, tuttavia, come un *cloud* del tipo *IaaS* come Ezzi Ltd., pur adottando la stessa identica formula di quella suesposta, non fa riferimento ai casi in cui può figurare da "controller". Al part. 15.1 è previsto solo il caso in cui sia *processor.* (http://www.ezzibiz.net/terms/)

ad una delle conclusioni di diversa dottrina in merito: la natura segmentata della qualificazione dei ruoli nel mondo *cloud*.[94]

5. I *CLOUD PROVIDER* SONO DAVVERO DEI *DATA PROCESSOR*?

Per quanto detto sinora, appare chiaro che i *cloud provider* svolgono (con riguardo ai *cloud-processed data*) se non una funzione di *controller,* almeno una funzione di *processor*[95], e su questo sembra essere ormai irremovibile l'Art. 29WP.[96]

Tuttavia è interessante esporre qui di seguito un intervento in letteratura che pone in discussione tale assunto.[97]

Da un'analisi approfondita della reale funzione svolta dal fornitore di servizio *cloud*, in effetti, traspare che lo stesso, seppur capace di intervenire in diverse fasi del trattamento dei dati, vive in una chiara asimmetria informativa riguardo al contenuto dei *cloud-processed data*.

Così come un venditore di computer che, ad esempio, si offre di gestire la manutenzione nel tempo per l'apparecchio venduto, non è in alcun modo *processor* dei dati che l'acquirente conserverà su quel computer, così anche un soggetto che dà in locazione il proprio computer, permettendo l'uso dei propri software e svolgendo una funzione di assistenza del prodotto e aggiornamento dei *software* nel tempo non è un *processor*.

Qualora, inoltre, tale locazione fosse permessa solo in locali di proprietà del locatore, e qualora fosse un'attività di grandi dimensioni (ad esempio una sala informatica) e il titolare indicasse il computer che più risponde alle esigenze del singolo utente, al punto che ogni utente possa personalizzare tale apparecchio ed averne utilizzo esclusivo ogni volta che si reca nella sala (salve sempre le funzioni di gestione, manutenzione, aggiornamento degli apparecchi da parte del titolare) egli non sarebbe comunque un *processor*, come non lo è un gestore di un *internet cafè*.

Anche nel caso in cui l'utente utilizzasse la potenza dell'*hardware* o l'insieme dei *software* in esso per sviluppare propri dati e propri *software*, non si potrebbe parlare di un proprietario-*processor* di quei dati.

Tale esempio può essere accostato ai *cloud* di tipo *Platform as a Service*.

Pur estendendo l'esempio alla circostanza in cui il titolare abbia diversi locali e diverse sale per il servizio sopra descritto, in cui gli utenti condividano gli stessi tavoli con dei *séparé* e in cui ci sia un servizio automatizzato che, ricordando le preferenze dei singoli utenti, indichi il tavolo, il locale e il computer riservato all'utente, semmai permettendo l'uso anche ai clienti dei miei clienti, o ai loro impiegati, o addirittura sia permesso ai suoi utenti di sub-locare i suoi computer, anche apportando modifiche o personalizzazioni non si potrebbe ancora parlare di attività di *processing* dei dati degli utenti da parte del gestore.

Tale esempio può essere confrontato ai *cloud* di tipo *Infrastructure as a Service*.

Ovviamente, quanto detto vale anche per il caso in cui tali computer abbiano un solo *software* installato (posta elettronica, *database*, ecc.) e sia permesso di apportare modifiche o personalizzazioni.

È l'esempio dei *cloud* di tipo *Software as a Service*.

---

[94] W.K. HON, C. MILLARD, I. WALDEN, *Who is responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Pt. 2, cit.*, 28.

[95] D. CATTEDDU, G. HOGBEN, *cit.*, 66; L.J. SOTTO, B.C. TREACY, M.L. MCLELLAN, *Privacy and Data Security Risks in Cloud Computing,* Electronic Commerce and Law Report, 2010, n.15, 186; R. GELLMAN, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, World Privacy Forum, 23 febbraio 2009, 19.

[96] Art. 29 Data Protection Working Party, *Opinion 05/2012 on Cloud Computing* (WP 196), 1 luglio 2012, 7-8; ma cfr. già Art. 29 Data Protection Working Party, *Opinion on "controller" and "processor", cit.*

[97] W.K. HON, C. MILLARD, I. WALDEN, *Who is responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Pt. 2, cit.,* 14-17.

La vera differenza tra gli esempi suesposti e i servizi *cloud* corrispondenti giace nella virtualizzazione dell'utilizzo e nelle diverse modalità di accesso degli utenti (fisico per le sale informatiche, in remoto per i *cloud*).

Tale differenza non può davvero fondare il passaggio da un ruolo di *non processor* ad un ruolo di *processor,* secondo la teoria qui esposta[98], anche perché la virtualizzazione ha sempre un fondamento fisico (*server*, *ram*, ecc.) che mantiene stabile il confronto sopra fatto, oltre al beneficio di una maggiore funzionalità ed efficienza del servizio.

Secondo questa ricostruzione, un solo caso può porre il dubbio che il *provider* sia un *processor*: i dati vengono conservati stabilmente sul *cloud* e il *provider* effettua anche dei *caching* per migliorare la velocità del servizio.

L'azione di conservazione o *storage*, infatti, è definita esplicitamente dalla legge tra le attività di *processing.*[99]

A questo punto si può sindacare sulla qualifica di "dati personali" attribuibile alle informazioni conservate dall'utente.

In effetti i dati possono essere resi anonimi dall'utente e dunque non più identificabili: un trattamento di questo tipo non soggiacerebbe ai vincoli della disciplina sui dati personali[100] e dunque il *provider* non sarebbe *processor*.

Il punto, dunque, è che un *provider* dovrebbe comportarsi diversamente a seconda che i dati siano resi anonimi, criptati o non lo siano, pur non avendo spesso gli strumenti per accedere ai dati e compiere tale distinzione.[101] È per questo che viene suggerita un'esenzione legislativa per i *cloud provider* dall'ambito di applicazione della disciplina, che si affianchi alla *household exemption* sopra illustrata.

Del resto, in grandi strutture di *cloud* i *provider* non hanno accesso ai dati nel momento in cui essi sono utilizzati dall'utente (è il caso del computer dato in locazione), e tuttavia quando non sono utilizzati dall'utente essi sono frammentati e scomposti in masse di dati anonime.[102]

Basterebbe, per giovare dell'esenzione, che il *provider* (come già avviene in alcuni casi) abbia preso tutti gli accorgimenti tecnici ed organizzativi affinché non siano riassemblabili i frammenti di dati se non dall'utente.

Gli accessi, inoltre, del provider al profilo utente sono solo incidentali e quindi inadatti a permettergli di riconoscere quali dati siano personali e quali non lo siano.[103]

Qualora, tuttavia, il *provider* agisca oltre i *terms of use* sottoscritti dall'utente ed in violazione della disciplina sui dati personali, egli rivestirebbe, come già detto, la funzione di *controller*, non già di *processor*.[104]

Resta il problema della poca trasparenza dei procedimenti interni ad un *cloud service* e dunque dell'ignoranza dell'utente (che a questo punto sarebbe *controller* e *processor*) rispetto ai terzi che fisicamente possono venire a conoscenza dei dati, risolvibile con accorgimenti interni ed architetturali da parte dei gestori del servizio.

L'esenzione di responsabilità proposta dovrebbe essere analoga a quella prevista per i "prestatori intermediari" (*mere conduit*, *caching* e *hosting*) alla sezione 4 della Direttiva sul commercio elettronico 2000/31/CE.[105]

---

98 W.K.HON, *et al., cit.*, 18.

99 Art. 2, lett. B, direttiva 95/46/CE; cfr. Anche art. 4, comma 1, lett. A codice della privacy e art. 4 Proposed Regulation.

100 Dunque non più nell'ambito di applicazione della direttiva, ai sensi del considerando n.26 (e n.23 della *Proposed Regulation).* Cfr. anche art. 3, codice della privacy. Cfr. W. K. HON, C. MILLARD, I. WALDEN, 'T*he Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1*' (2011) Queen Mary School of Law Legal Studies Research Paper No 75/2011 ('CLP Personal Data Paper').

101 Al contrario gli utenti possiedono tali informazioni e spesso sono anche tutorati nell'utilizzo dei *cloud service* nell'operazione di criptaggio dei dati, cfr. R, MASON, *Data Security and the Nasuni Filer – Just the Facts*, Nasuni blog, 15 March 2010, http://www.nasuni.com/blog/120-data_security_and_the_nasuni_filer-just_the_facts (consultato il 15 ottobre 2013).

102 W.K. HON *et al.*, *cit.*, 22.

103 *Ibidem.*

104 Cfr. *Supra* par. 2 e nota 13.

Tuttavia, la succitata direttiva all'art. 1, comma 4, lett. B, esclude espressamente la sua applicazione negli ambiti già regolati dalla direttiva sulla protezione dei dati.

È ovvio, comunque, che entrambe le direttive furono scritte e concepite in un periodo in cui il *cloud computing* non esisteva, né potevano esserne previsti i grandi successi e potenzialità[106]: non si immaginava che potessero esserci delle attività che seppur nell'ambito di un trattamento di dati personali, potessero presentare esigenze analoghe a quelle di un prestatore intermediario.

In effetti, così come un servizio di *hosting* o *mere conduit* ha un certo grado di esenzione di responsabilità nella misura in cui non conosce le informazioni trasmesse[107], così un *cloud* (e un *internet café*) dovrebbero giovare della stessa esenzione, sulla base di un principio di "conoscenza e controllo".[108]

Tuttavia, una specifica esenzione per i *cloud provider* rischia di cadere al di fuori della neutralità tecnologica della normativa, incorrendo nelle censure del garante europeo.[109]

Un'altra strada sarebbe quella di abolire il dualismo *controller/processor*, ai fini di una responsabilità chiara e unitaria (detta "*end-to-end responsibility*").

Tale principio, peraltro, è stato già abbozzato dalla Commissione Europea[110] che ha definito inadatto l'attuale quadro normativo a trattare il contesto del *cloud computing*, laddove è invece preferibile una responsabilità *end-to-end*, che gioverebbe all'affidabilità del servizio[111], specificando sempre per quale operazione è responsabile in prima persona un soggetto anziché un altro, con evidenti benefici anche sul piano dell'esportazione dei dati all'estero.[112]

Tali auspici e osservazioni, tuttavia, sono rimasti disattesi anche dalla *Proposed Regulation.*[113]

Comunque, al di là di auspici per modifiche legislative future, occorre determinare oggi, alla luce della legge vigente e dei provvedimenti in corso di approvazione, quale sia la migliore soluzione al riguardo per la *privacy* nel mondo dei *cloud,* posto che i *cloud providers* svolgono un'azione (lo *storage*) che concretamente rientra negli ambiti del *processor.*[114]

Tra le novità del regolamento che potrebbero aiutare ad uscire dall'impasse, spicca la maggiore definizione della funzione del "*joint*" *controller* o *processor*, con i conseguenti requisiti per la sua identificazione.[115]

IV. LA FIGURA DEI *SUB-PROCESSORS*

Un altro problema rilevante nell'ambito dell'assetto economico-strutturale del *cloud service* è la prassi aziendale, ormai sempre più radicata, di demandare il trattamento dei dati personali in *outsourcing* a soggetti esterni all'azienda.[116]

---

[105] C. MILLARD, *et al.*, *Response to the UK Ministry of Justice's Call for Evidence on the European Commission's Data Protection Proposals, Cloud Legal Project*, Queen Mary, University of London, 2012, (http://www.cloudlegal.ccls.qmul.ac.uk/docs/65220.pdf),.3

[106] Article 29 Data Protection Working Party and Working Party on Police and Justice, *The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, cit., 41.

[107] I. WALDEN, '*Mine host is searching for a "neutrality" principle!*', Computer Law and Security Report, 2010, n.26, 203.

[108] W.K. HON, *Who is responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Pt. 2 , cit.*, 28.

[109] Cfr. European Data Protection Supervisor, *Additional Comments on the Data Protection Reform Package, cit.,* par.39.

[110] Cfr. The European Commission's Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data: Alcatel-Lucent contribution (2009), (http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/alcatel_lucent_en.pdf), 5.

[111] Il principio della *accountability* è stato lungamente discusso (Cfr. Article 29 Working Party, *Opinion 3/2010 of 13 July 2010 on the principle of accountability* (WP 173)) e definitivamente introdotto nel Capo IV della *Proposed Regulation,* cfr. European Data Protection Supervisor (P. HUSTINX), *Opinion on the Data Protection Reform Package*, 7 marzo 2012, par. 166.

[112] W.K. HON *et al.*, *ult.op.cit.*, 25-26.

[113] C. MILLARD, *et al.*, *Response to the UK Ministry of Justice's Call for Evidence on the European Commission's Data Protection Proposals, Cloud Legal Project*, cit., 9: "*The either processor or controller (or both) model is maintained. A more nuanced definition of processor, or an exemption for those cloud service providers who are passive intermediaries, would be welcome*".

[114] Nota 64.

[115] vd. *Infra* Par. 5.

[116]W.K. HON *et al*, cit., 27; cfr. anche Art. 29 Working Party, *Opinion 05/2012, cit.*, 9.

Tale delega può essere svolta sia dal *controller*, in modo che non ci siano difficoltà nel definire "*processor*" i soggetti terzi, sia dagli stessi *processor* che attraverso un sub-contratto deleghino parte delle attività trattamento dei dati a loro affidato a soggetti esterni, col conseguente frazionamento della figura del *processor*.[117]

Chiaro è che tale situazione aggrava le incertezze applicative della disciplina sul trattamento dei dati, come specificato dalla stessa Commissione.[118]

Sebbene la direttiva europea 95/46/CE non preveda figure di "*sub-processor*", nella disciplina italiana tale fenomeno può ritenersi (seppur solo in parte, *vd. infra*) compreso nel riferimento all'"incaricato" del trattamento di cui all'art. 4, lett. h e all'art. 30 del Codice della privacy.

Tuttavia, dalla dizione letterale delle disposizioni appare chiaro che tale previsione è limitata alle "persone fisiche"[119] e che le stesse devono operare sotto la diretta autorità del *controller* o del *processor* attenendosi alle istruzioni impartite[120], nell'ambito di un rapporto di preposizione.[121]

Del resto, la *ratio* dell'istituto va rinvenuta nell'esigenza di agevolare le strutture di medie e grandi dimensioni rispetto ai limiti previsti dal Codice della privacy per la comunicazione di dati a soggetti terzi e per il trattamento di dati da parte di questi ultimi, che impedirebbero un'efficiente azione del nucleo organizzato[122], in ossequio ad un principio di "libertà informatica"[123], e non già di regolare fenomeni di *outsourcing* delle funzioni del *processor* ad eventuali persone giuridiche *sub-processors.*

Inoltre, la dottrina ha ritenuto che l'incaricato dovesse essere esplicitamente un lavoratore dipendente di una delle figure incaricate[124] o, come ha chiarito il Garante[125], anche un lavoratore autonomo, collaboratore esterno o soggetto altrimenti autorizzato, purché *de facto* equiparabile ad un dipendente quanto alle funzioni svolte[126], ma mai una persona giuridica (come può essere un'azienda terza), perché la stessa, se delegata al trattamento, può fungere soltanto da *processor*[127].

Per la verità, in dottrina si è già riflettuto sulla possibilità di una corresponsabilità (o, più chiaramente, di un *joint-processing*) tra *processor* e "incaricato" (persona fisica), qualora questi sia deputato non già al trattamento materiale, ma alla gestione del trattamento, ai sensi della struttura di rapporti disegnata dalla normativa italiana. Tuttavia, tale soluzione è stata esclusa poiché per la qualifica di *processor* si è ritenuta una condizione necessaria la designazione diretta da parte del *controller,* che infatti risponde per *culpa in eligendo ex* art. 29 codice della privacy (mentre l'incaricato opera solo sulla base di una organizzazione interna del *processor)* e poiché tale soluzione svilirebbe l'opportunità che il *processor* sia anche un ente associativo, dal momento che tutto sarebbe ridotto all'incaricato-persona fisica. Ciononostante, non può trascurarsi che in questo caso il responsabile perderebbe comunque l'incisività che il codice sembra volergli attribuire in relazione al suo contatto diretto col trattamento dei dati, contatto perso nell'organizzazione interna dell'ente.[128]

---

117 Art. 29 Working Party, *Opinion 05/2012, cit*., 9.

118 Commissione Europea, *Communication to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the regions, Unleashing the Potential of Cloud Computing in Europe*, 27 settembre 2012, 8-9.

119 Art. 4, lett. h. Cfr. S. MELCHIONNA, *I principi generali,* in *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice,* a cura di Acciai, Santarcangelo di Romagna, 2004, 64.

120 Art. 30, comma 1.

121 V. GAGLIARDI, *Commento all'art. 30 - Incaricati del Trattamento,* in *La protezione dei dati personali*, *Commentario al D.Lgs. 30 giugno 2003, n. 196 «Codice della privacy»*, a cura di C.M. Bianca e F.D. Busnelli, Padova, 2007, 673.

122 *Ibidem*, 666.

123 S. FADDA, *commento all'art. 19,* in *La tutela dei dati personali. Commentario alla legge 675/1996*, a cura di E. Giannantonio, M.G. Losano, V. Zeno-Zencovich, Padova, 1997, 190. Cfr. al riguardo il principio della "libertàà d'impresa" in campo informatico, rimarcato *ex multis* da Corte di Giust. Europea, sent. 24-11-11 causa C-70/10 (caso *Scarlet Extended*).

124 S. FADDA, *cit*., 192; P.M. VECCHI, *Art. 4 - Definizioni*, in *La protezione dei dati personali*, *Commentario al D.Lgs. 30 giugno 2003, n. 196 «Codice della privacy», cit*., 73.

125 Cfr. il parere del Garante per la Protezione dei Dati Personali del 2 dicembre 1997, reso al Consiglio Superiore della Magistratura, in *Bollettino*, 1997, n. 2, 40.

126 V. GAGLIARDI, *ult.op.cit.*, 671.

127 V. il parere del Garante con nota dell'8 giugno 1999, in *Bollettino*, 1999, n.9, 58.

128 P.M. VECCHI, *cit*., 73.

Tuttavia, la particolarità della disciplina italiana rispetto alla direttiva europea è stata salutata con plauso, dato che essa evita di appiattire e confondere il ruolo della persona fisica che tratta i dati rispetto all'ente (solitamente) associativo preposto al trattamento materiale dei dati e da cui la persona fisica riceve l'incarico.[129]

Inoltre, la disciplina italiana risulta apprezzabile per gli oneri di chiarezza richiesti nel rapporto tra responsabile e incaricato poiché si prevede che la designazione avvenga per iscritto[130] e individua puntualmente l'ambito del trattamento consentito (art. 30, comma 2), evitando così i rischi di complessità di ruoli e conseguente diluizione della responsabilità.[131]

Va, tuttavia, rilevato che la *Proposed Regulation* all'art. 26 chiarisce in modo dettagliato gli obblighi sia del *processor* che dei *sub-processor*.[132]

Comunque, un rischio molto forte nel *cloud computing* (soprattutto nella sua declinazione *Infrastracture as a service* e nello specifico nel c.d. *grid computing*[133]) può essere la presenza di una pluralità di *processor* per segmenti diversi di uno stesso trattamento.

È per questo che l'Art. 29 WP raccomanda che nel contratto di *cloud* le responsabilità e i ruoli siano allocati chiaramente e non dispersi attraverso una catena di *outsourcing* / *subcontracting*, salvo che le responsabilità all'interno della catena siano chiaramente stabilite[134].

Già la Commissione Europea, nel 2010,[135] nel modello di clausole *standard* per il trasferimento di dati personali a *processor* stabiliti in paesi extra-europei, permetteva il *sub-processing* solo col preventivo consenso scritto del *controller* e con un accordo scritto che imponesse al *sub-processor* le stesse obbligazioni gravanti sul *processor*. Tale previsione è stata poi puntualizzata all'art. 26(2) della *Proposed Regulation*.

Secondo l'Art.29 WP, il *processor* può concludere dei sub-contratti sulla sua attività attraverso due modalità: nomina tutti i *sub-processor* (anche eventuali) nel contratto originario con l'utente, oppure obbliga i *sub-processor* ad adempiere agli stessi termini contrattuali del contratto originario (notificando sempre il tutto all'utente). [136]

Inoltre si ritiene che il *controller* debba poter ricorrere contro ogni violazione del contratto compiuta dai *sub-processor*: ciò deve essere reso possibile o attraverso una responsabilità indiretta del *processor* oppure introducendo il *controller* tra le parti contrattuali (in qualità di terzo beneficiario o di mandante del *processor*).[137]

---

129 *Ibidem*, 72-73; S. MELCHIONNA, *ult.op.cit*., 64.

130 Non sono mancate, tuttavia, al riguardo le critiche già sopra accennate riguardo all'aumento di burocratizzazione nella gestione d'impresa derivante dell'onere della forma scritta. Cfr. Ri. IMPERIALI e Ro. IMPERIALI, *La tutela dei dati personali, cit*., 80.

131 Cfr. C.DI COCCO, *Soggetti che effettuano il trattamento*, in *Il Codice in materia di dati personali*, *cit*., 134; Tale rischio è sentito fortemente anche dall'Art.29 Data Protection Working Party, Opinion 05/2012, *cit*., 8.

132 G. BUTTARELLI, *cit*., 6.

133 Cfr. Art. 29 Data Protection Working Party, Communication on controller and processor, *cit*., 28 sulle qualifiche nel *grid computing*.

134 *Ibidem*, 29; anche Art. 29 Working Party, *Opinion 05/2012, cit*., 9.

135 Decisione della Commission Europea del 5 febbraio 2010, 2010/87EU, art. 3, lett. E, e considerando nn. 16-22.

136 Art.29 Data Protection Working Party, *Opinion 05/2012*, *cit*., 10.

137 *Ibidem*. Si noti, tuttavia, che le conseguenze sulla tutela del *controller* appaiono diverse a seconda che il *controller* sia terzo beneficiario del contratto di *subprocessing* (ex 1411 ss. c.c.) oppure mandante del processor (in analogia al rapporto di mandato che intercorre tra *controller* e *processor*, vd. *supra*, Par. 2*)*. Nel primo caso, in effetti, il controller non è propriamente una parte contrattuale, pur potendo esigere l'esecuzione direttamente dal *subprocessor* (a differenza del caso sopra descritto di responsabilità indiretta del *processor*). Nel secondo caso, invece, se il contratto tra *controller* e *processor* fa espressa menzione di eventuali rapporti di *subprocessing* può parlarsi di mandato con rappresentanza (con tutti gli obblighi conseguenti per il *controller*-mandante, *ex* artt. 1719 e 1720 c.c.), altrimenti si tratterebbe di mandato senza rappresentanza (*ex* art. 1705 c.c.) più simile al primo caso (il *controller* non è direttamente parte del rapporto, tuttavia può esigerne le prestazioni).

Nel nostro ordinamento, per continuare il parallelo con la figura dell'"incaricato", vd. *supra*, nell'ambito della responsabilità extra-contrattuale, pur essendo fuori di dubbio la responsabilità indiretta del *processor* per i danni cagionati dal suo delegato-incaricato *(*in forza dell'art. 2049 c.c.) trattandosi di rapporto di preposizione, non è comunque esclusa la responsabilità del preposto (cfr. C.M.BIANCA, *Diritto Civile 3*, *cit*., 730, nota 7 e C. SALVI, *Responsabilità extra-contrattuale (diritto vigente)*, in *Enc.Dir.*, Milano, vol XXXIX, 1243 e ss.; V. GAGLIARDI, cit., 677).

Il nuovo Regolamento in via di approvazione, infine, prevedendo la qualifica di *joint processor* o *coincaricato*[138], apre la strada al riconoscimento di una pluralità di persone (fisiche o giuridiche che siano) che si occupino del trattamento materiale dei dati personali, tuttavia, la previsione dell'art. 77 riguardo alla responsabilità per danno da trattamento illecito rende esiziale una distinzione gerarchica tra *processor* e *subprocessor*, poiché prevede un regime di responsabilità solidale tra tutti i soggetti che si occupino del trattamento (sia dettando scopi e modalità, sia eseguendo gli stessi).

V. SOLUZIONI E NOVITA NELLA *PROPOSED REGULATION*: UN "*PROCESSOR*" CON PIÙ OBBLIGHI E IL NUOVO "*JOINT-CONTROLLER*"

Da quanto finora detto si può concludere che la disciplina vigente, dettata dalla direttiva 95/43/CE, è inadatta a rappresentare i reali rapporti economico-commerciali intervenenti nel *cloud computing*.

Tuttavia, tale conclusione oltre a scontrarsi con la necessità imprescindibile di risolvere i rapporti tra i soggetti che effettuano il trattamento, onde evitare che le difficoltà identificatorie si riverberino negativamente sui soggetti titolari dei dati, obbliga ad esaminare se la *Proposed Regulatio*n, elaborata in un contesto socio-tecnologico in cui il *cloud* è ormai una realtà consolidata, risolverà la situazione o al contrario perpetuerà i problemi previgenti.

Essa va in due direzioni: da un lato implementa gli obblighi e la centralità del *processor*, pur creando nuovi obblighi per il *controller*[139], dall'altra prevede con maggiore chiarezza la figura del *co-controller*. Dato comune è il superamento definitivo del dualismo *controller/processor*.

In effetti, la *Proposed Regulation* estende alcuni obblighi originariamente del *controller* anche al *processor*. Tale novità sembra sia stata prevista proprio per tenere conto della centralità crescente del ruolo del *provider-processor* nel trattamento, soprattutto nel determinare alcune condizioni essenziali dello stesso, come nel contesto del *cloud computing,* in cui l'asimmetria del rapporto con l'utente si affianca alla diffusa pratica del *sub-processing*.[140]

Nello specifico, l'art. 26 prevede una serie di obbligazioni, ad esempio che il *processor* aiuti il *controller* ad adempiere alle richiese in merito alla sicurezza (lett. F), anche creando le condizioni ottimali per l'azione (lett. E), compia una valutazione dell'impatto del trattamento dei dati (lett. C e art. 30, 1° comma) e mantenga una aggiornata documentazione delle operazioni (art. 28).

Sembra dunque che nelle intenzioni del legislatore europeo traspaia la volontà di riservare al *cloud provider* il ruolo di *processor*. Rimarrebbero tuttavia i problemi definitori sopra affrontati: ci troveremmo di fronte ad un utente/*controller* pur sempre vittima di un rapporto asimmetrico.[141]

Tuttavia, su tale innovazione gravano molti emendamenti abrogativi[142] che mirano a mantenere la responsabilità del *processor* ai livelli minimi previsti dalla direttiva vigente. Il Garante Europeo si è già dichiarato contrario a tali emendamenti.[143]

---

[138] L'art. 77, 2° comma recita "qualora il trattamento coinvolga (...) più incaricati"; e implicitamente l'art. 13 estende i diritti dei destinatari in base all'articolo 12, lettera c), della direttiva 95/46/CE anche al co-incaricato, come da Relazione alla Proposta di Regolamento, par. 3.4.3.

[139] Tale ampliamento di obblighi per il controller deriva dall'irrobustimento della tutela nei confronti dell'interessato. Tra tutti, bisogna rilevare il diritto all'oblio (art. 17, Proposed Regulation) e alla portabilità dei dati (art. 18), oltre che la previsione generale di un obbligo per il *controller* di stabilire procedure per assicurare l'effettivo esercizio dei diritti dell'interessato (art. 12). Cfr. G. BUTTARELLI, *Security and privacy regulatory challenges in the Cloud*, cit.

[140] European Data Protection Supervisor, *Additional Comments on the Data Protection Reform Package*, Brussels, 15 marzo 2013, par. 25. Riguardo ai "sub-processor" vd. *supra*, par. 4.

[141] vd. par. 3.5

[142] ITRE AM 43, 229, 231, 233, 238, 260; LIBE AM 1808-1810, 1829, 1832, 1834, 1836, 1837, 2024.

[143] European Data Protection Supervisor, *Additional Comments on the Data Protection Reform Package*, Brussels, 15 March 2013, Par. 25.

Altra strada percorribile consisterebbe nello sdoganare il rapporto binario *controller/processor*, per affiancare all'utente un corresponsabile: l'art. 24 della *Proposed Regulation* prevede esplicitamente una figura solo accennata dalla direttiva previgente, il *joint controller*.

La direttiva 95/46/CE, infatti, prevedeva all'art. 2, lett. d che il *controller* determinasse le finalità e gli strumenti del trattamento "da solo o insieme ad altri"[144]. Da notare, tra l'altro, che tale riferimento non era contenuto nella Convenzione 108[145], ma è stato aggiunto in sede di direttiva.

Tuttavia, non si chiariva la ripartizione della responsabilità tra i diversi *controller* né tantomeno se tutti gli "altri" indicati nell'inciso della disposizione fossero *controller* di pari grado oppure dovessero essere considerati in ruoli intermedi, sussidiari o secondari.[146]

In realtà, la Commissione Europea in un'opinione preparatoria all'approvazione della direttiva interpreta tale disposizione considerando solo il caso in cui tutti i *co-controller* determinino egualmente (e dunque contestualmente) scopi e mezzi e siano egualmente responsabili per lo stesso singolo trattamento.[147]

La norma così interpretata, ovviamente, non giova al complesso rapporto di ruoli e funzioni intercorrenti nel *cloud computing*, dove è proprio una differenziazione di soggetti a svolgere funzioni diverse, seppur rientranti nell'ambito del *controller*.[148]

La stessa definizione di "trattamento" fornita sia dalla direttiva[149] sia dal regolamento,[150] del resto, è così vasta da includere implicitamente una diversità di fasi e quindi di soggetti.

Secondo l'Art.29 WP si può parlare di "*joint controller*" qualora parti diverse, riguardo a specifiche operazioni di trattamento, determinino lo scopo o gli altri elementi essenziali del trattamento, sia che si tratti di una stretta collaborazione, sia che si tratti di un rapporto più slegato.[151]

La *Proposed Regulation* definisce i *joint controller* ("corresponsabili del trattamento") come coloro che congiuntamente determinano le finalità, le condizioni e i mezzi del trattamento dei dati personali mediante un accordo interno (art. 24).

Dato che la ripartizione di responsabilità e funzioni rischia di affievolire l'effettività della disciplina, è necessario che l'allocazione dei ruoli e delle competenze sia chiara e diretta, così come i diritti che il soggetto può esercitare verso un *controller* piuttosto che verso un altro.[152]

Ciò è stato ancor più fortemente rimarcato dalla Risoluzione Legislativa del Parlamento Europeo che ha emendato la *Proposed Regulation*: al considerando 62, infatti, è stato aggiunto che "occorre che gli accordi tra i corresponsabili del trattamento riflettano i loro ruoli e rapporti effettivi. È necessario che il trattamento dei dati personali a norma del presente regolamento preveda la possibilità per un

144 Cfr. G. BUTTARELLI, *Banche dati e tutela della riservatezza,* Milano, 1997, 168.

145 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Consiglio Europeo, 28 gennaio 1981.

146 Art. 29 Data Protection Working Party, *Opinion on "controller" and "processor", cit.,* 18. In dottrina si rilevava soltanto che (Cfr. P.M. VECCHI, *cit*., 70) il riferimento alla contitolarità del trattamento andasse identificato nella comunanza della possibilità di determinare finalità modi del trattamento medesimo derivante dalla compartecipazione finale degli interessi in vista della cui soddisfazione viene predisposto il trattamento dei dati personali.

147 Opinion of the Commission pursuant to Art. 189 b (2) (d) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a EP and Council Directive on the protection of individuals with regard to the processing of personal data and of free movement of such data, 18 luglio 1995, COM(95) 375, 3: *"For a single processing operation a number of parties may jointly determine the purpose and means of processing to be carried out"* e perciò in questo caso *"each of the co-controllers must be considered as being constrained by the obligations imposed by the Directive so as to protect the natural persons about whom the data are processed"*.

148 Vd. supra, § III. D.

149 Art. 2, lett. b: "...la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione..."

150 Art. 4, comma 3, *Proposed Regulation.*

151 Art. 29 Data Protection Working Party, *Opinion on "controller" and "processor", cit.,* 19.

152 *Ibidem,* 18.

responsabile del trattamento di trasmettere i dati a un corresponsabile o a un incaricato del trattamento affinché esegua il trattamento per suo conto".[153]

Peraltro, nello stesso articolo 24 è specificato che il rapporto tra questi e il *controller* principale (con la relativa ripartizione di responsabilità e relazione con il soggetto interessato) è risolto tramite accordi interni stipulati tra le due parti, in cui siano esplicitate le rispettive responsabilità in merito all'adempimento degli obblighi derivanti dal regolamento, con particolare riguardo alle procedure e ai meccanismi per l'esercizio dei diritti dell'interessato.

Anche qui il legislatore europeo si è preoccupato di specificare, rispetto alla formulazione originaria che l'accordo riflette adeguatamente i rispettivi ed effettivi ruoli dei corresponsabili e i loro rapporti nei confronti degli interessati.[154]

Da ciò si deduce che il contratto di *cloud* diventa quindi un mero "accordo interno" *ex* art. 24. Non essendo infatti richiesti tutti gli oneri di forma e di contenuto espressi all'art. 17 della previgente direttiva, non sembra costituire più un problema la circostanza che tale contratto sia in realtà un formulario *standard*.

Tuttavia, possono rinvenirsi nella Proposed Regulation alcune indicazioni di disciplina in merito all'accordo tra i *joint controllers*: innanzitutto nella riformulazione emendata dell'art. 24 è stabilito che il contenuto essenziale dell'accordo deve essere "messo a disposizione dell'interessato".[155]

Inoltre, in tema di responsabilità l'art. 77 prevede che, a prescindere dalle diverse ripartizioni interne di responsabilità, *controller, joint controller, processor e joint processor* del trattamento rispondano in solido per l'intero ammontare del danno eventualmente cagionato per il trattamento dei dati, "*a meno che non sussista un adeguato accordo scritto tra di essi che stabilisce le responsabilità a norma dell'art. 24*".[156] Da un'analisi testuale della norma si può affermare che il termine "adeguato" non va inteso in senso generale, ma solo relativamente alla ripartizione delle responsabilità: è "adeguato" a questi fini un accordo che abbia una chiara allocazione delle responsabilità in chiave di danno.

Possiamo perciò concludere che tale accordo, seppur a forma e contenuto liberi, va comunicato (e dunque scritto) almeno nelle sue parti essenziali all'interessato e dev'essere "scritto" e "adeguato" (nel senso sopra specificato) a pena dell'applicazione del principio della responsabilità solidale.

Infine l'art. 13 prevede in capo ai *joint controllers* il diritto di ricevere comunicazione dal *controller* di tutte le modifiche o cancellazioni di dati avvenute nell'esercizio dei diritti alla rettifica (art. 16) e all'"oblio e cancellazione" (art. 17) da parte dell'interessato[157].

Mentre il primo di questi diritti era già presente nella normativa previgente[158] il secondo è una parziale novità[159] della *Proposed Regulation* assieme al diritto alla portabilità (art. 18).

La previsione di "nuovi diritti", in effetti, comporta nuovi obblighi in capo al *controller*, e dunque uno sbilanciamento della struttura dei rapporti a svantaggio del *controller*. Tuttavia occorre che tali obblighi siano ripartiti tra i vari *joint controller*, in base all'effettivo ambito decisionale di cui hanno potere nel trattamento. In effetti, il *provider* è nella posizione migliore per adempiere al secondo comma dell'art. 17[160] e potenzialmente anche al settimo comma[161] dato il carattere "tecnico" delle disposizioni, ma solo

---

153 Risoluzione legislativa del Parlamento Europeo del 12 marzo 2014 sulla 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 (regolamento generale sulla protezione dei dati) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), emendamento 38.

154 *Ibidem,* emendamento 119.

155 *Ibidem,* emendamento 119.

156 *Ibidem*, emendamento 187.

157 "Salvo che ciò si riveli impossibile o implichi risorse sproporzionate" (art. 13).

158 Art. 6 lett. D, direttiva 95/46/CE; art. 7, comma 3, "Codice della Privacy".

159 Era previsto un diritto alla cancellazione anche nella direttiva 95/46/CE, all'art. 12, lett. B, tuttavia l'attuale diritto "all'oblio e alla cancellazione" è ben diverso, in quanto più ampio e dettagliatamente descritto. Cfr. al riguardo EDPS, *Opinion on Data Protection Reform Package*, *cit*., par. 146.

160 "Quando ha reso pubblici dati personali, il responsabile rende tutte le misure ragionevoli, anche tecniche, in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali". Il riferimento ai "terzi" sembra calzare perfettamente con le figure dei *sub-contractors* di cui si servono i *provider*.

colui che stabilisce le finalità per il trattamento (l'utente) può verificare se sussistano le condizioni per la cancellazione di cui al comma 1 o i motivi esimenti di cui al comma 3 e 4. È questo un chiaro esempio dell'efficacia e utilità del *joint-controlling* nel trattamento dei dati.

Comunque, sebbene il *provider* spesso non sia in grado, come sopra specificato,[162] di assicurare l'adempimento di tutte le obbligazioni del *controller*, ciò non implica un'automatica esclusione dalla qualifica di *controller*.[163]

Questo nuovo disegno sembra particolarmente indicato per i concreti rapporti nel mondo *cloud*.

In effetti, rifletterebbe meglio il livello di influenza reciproca che intercorre tra le parti, con una più realistica allocazione di responsabilità. Ciò, però, va tenuto in considerazione nella negoziazione dei *Terms of Service*, che dovrebbero per esempio indicare chiaramente quale controller è responsabile per quale fase nel trattamento e in base a quali obbligazioni ai sensi disciplina della protezione dei dati.[164]

Di conseguenza, l'utente dovrebbe essere reso responsabile per le fasi di trattamento su cui svolge un effettivo controllo. Resta, comunque, il problema dell'asimmetria contrattuale al momento della conclusione del contratto di *cloud*, ma tale problema sembra superabile attraverso l'uso di termini e condizioni contrattuali *standard* accorti e bilanciati.[165]

Tale soluzione, peraltro, risolve anche il già menzionato problema della non identificabilità delle persone giuridiche tra i "soggetti" interessati dal trattamento, senza obbligare le persone giuridiche ad essere sempre e comunque uniche "*controller*" del trattamento.[166]

VI. CONCLUSIONI: OLTRE LE BARRIERE DEL DUALISMO

La conclusione che, da queste pagine, si impone con maggiore vigore riguarda l'inadeguatezza della normativa vigente rispetto alla complessità della tecnologia del cloud computing.

Una rete di asimmetrie domina il rapporto rendendo difficile ogni definizione aprioristica: un'asimmetria contrattuale (e strutturale) impedisce all'utente di calzare perfettamente il ruolo di data controller; un'asimmetria informativa (riguardo ai *cloud-processed data*) rende spesso difficile al provider anche la mera qualifica di *processor*.

Per riportare equilibrio nel rapporto, occorre far tesoro del portato del Regolamento in corso di approvazione: bisogna rompere definitivamente il dualismo *controller/processor*, puntando sulla nuova figura trasversale del joint-controller, Tale figura va accompagnata ad un chiaro regolamento di rapporti tra i "responsabili", affinché ciascuno risponda per ciò di cui ha poteri e strumenti informativi, e il soggetto interessato dal trattamento dei dati sappia sempre a chi rivolgersi per l'esercizio di un particolare diritto.

Non va neppure sottovalutata la nuova figura del *processor* delineata dal regolamento. Essa rende comunque più accettabile l'attribuzione dello status di *processor* al *provider*, dati i maggiori obblighi a lui richiesti.

---

161 "Il responsabile del trattamento predispone i meccanismi per assicurare il rispetto dei termini fissati per la cancellazione dei dati personali e/o per un esame periodico della necessitàà di conservare tali dati". Il richiamo ai "meccanismi" e ad un "esame periodico" appare particolarmente indicato per la struttura del servizio di *cloud*.

162 Vd. paragrafo 3.6

163 Art. 29 Data Protection Working Party, *Opinion on "controller" and "processor", cit.,* 22.

164 European Data Protection Supervisor (P. HUSTINX), *Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"*, 16 novembre 2012, par. 55.

165 In base alle indicazioni suggerite da European Data Protection Supervisor, ult.op.cit., alla Sezione V.3: "*Developing model contract Terms and Conditions"* (parr. 118-115); cfr. anche i parametri per l'efficacia del contratto tra utente e cloud provider in Art. 29 Data Protection Working party, *Opinion 5/2012*, cit., 12-13.

166 Cfr. nota 61.

La chiave di volta è sicuramente rappresentata dai contratti di *cloud*. Essi devono essere chiari, specifici e dettagliati, cosicché eventuali sub-contratti non costituiscano ostacolo all'esercizio dei diritti degli utenti.

La meta sarebbe, com'è chiaro, termini contrattuali standard europei che risolvano chiaramente, a seconda del diverso tipo di *cloud* e di dati: funzioni, responsabilità, obblighi e diritti.

Superando i formalismi delle definizioni, ma con approccio funzionalistico, lo scopo finale dev'essere, come sempre, quello di incentivare le grandi potenzialità del *cloud*, senza perdere di vista che nella complessità tecnologica la tutela per i diritti dell'interessato deve restare alta.