ISSN: 2281-5147

Opinio Juris in Comparatione

Studies in Comparative and National Law

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

The EU's Right to Be Forgotten as Applied to Cloud Computing in the Context of Online Privacy Issues

by

Francesco Lazzeri

www.opiniojurisincomparatione.org

THE EU'S RIGHT TO BE FORGOTTEN AS APPLIED TO CLOUD COMPUTING IN THE CONTEXT OF ONLINE PRIVACY ISSUES

by

Francesco Lazzeri[*]

Abstract:

The core of this study concerns the implementation of Art. 17 of the EU Proposal for a General Data Protection regulation, introducing a «right to be forgotten and to erasure», in light of the essential features of cloud computing services.

In a wider perspective, the fundamental issues underlying this problem can be summed up as follows: how can personal information be deleted from the Internet? And, most important: when is it admittable to do so?

As a matter of fact, both these questions can be specified by inquiring on whether full erasure is materially and technically possible and on which conditions and legal boundaries such an action should face.

It has emerged that Art. 17, believed by many to be inappropriate already with reference to the expression «right to be forgotten», is not adequate to provide a satisfying response in terms of transparent regulation and efficient protection of relevant interests.

A practical paradox arises: in fact, those very characteristics of the web that make it so appealing and economically profitable prove themself as one of the main obstacles when it comes to effectively deleting information. The Internet, it has been said, has indeed an eternal memory.

Besides the practical issues of removing copies and links from the web, the article focuses on the legal framework protecting the interest of data subject to the erasure of personal information.

Under this aspect, a convincing evaluation of the currently applicable data protection rules comes from the Advocate General's Opinion in a recent case (*Google vs. Spain*, C-131/12), on which the Court of Justice has only recently rendered its judgment, of which the article gives a first evaluation.

The AG has concluded that individuals cannot derive a general «right to be forgotten» from Directive 95/46. The following decision by the Court — mostly in light of artt. 7 and 8 of the Charter of

[*] Graduate law student at Sant'Anna School of Advanced Studies in Pisa.

Fundamental Rights of the European Union — while establishing that search engines must delete "inadequate, irrelevant or no longer relevant" data from their results, made clear that in order for "delisting" to be conceded, the proper balance has to be stricken by the search engine itself between fundamental rights and public interest in continued ability to access information, thus making the implementation of such a right unsystematic and potentially arbitrary.

In contrast, a first glance at the Proposal for a General Data Protection Regulation may suggest that a major overhaul has been performed. However, when looked at more closely, Art. 17 do not seem to represent a substantial change. In fact, the hypothesis enabling erasure can be brought back to the cases of (a) data retention in contrast with the law and of (b) supervening lack of reasons legitimating data processing.

The Author's opinion is that the real innovation, if any, consists in the role acknowledged to consent, which, according to Art. 7 of the Proposal, can be now withdrawn «at any time».

It is not easy to understand how some of the grounds for erasure will adapt to the cloud dimension.

There is a major problem to be highlighted as prejudicial to the implementation of Art. 17 in the context of cloud computing services: the most critical aspect about this provision is (first) defining and (then) identifying the subjects involved. That means, understanding who is the controller and who is the processor in each situation, as well as their relationship with the data subject.

Compared to par. 1, the second paragraph of Art. 17 is more appreciable in the sense that it is implicitly devised with a view to the structure of the Internet and of Internet services: therefore, it is probably the more interesting when dealing with cloud computing. Even so, it is hard to understand how it can be implemented, for two main reasons which are:

(a) First, if we agree with Art. 29 WP's opinion, we should identify the controller with the cloud client; but this solution ignores the fact that the user usually does not have a range of technical tools comparable to the one of the provider. In contrast, qualifying the cloud provider as the data controller would lead to a better allocation of responsibility.

(b) Secondly, it is unclear what will happen once third parties have been informed of the data subject's request to obtain erasure. Par. 2 remains silent on the point, but it is easy to realize that similar situations may be very frequent (if not the most frequent).

In addition, in order to understand the scope and limits of a «right to be forgotten» in the current information age, the Author tries to pick up the relevant clues laid down by the Court of Justice in relation to cases involving ISP, on the assumption that the cloud provider can be intended as such.

In this regard, the Proposal could play a key role in promoting privacy-oriented technologies, especially by means of the implementation of two principles: privacy by default and minimization of data collection.

In conclusion, if Art. 17 entries into force as it is now, a number of problem would arise concerning its true scope; in particular, how cloud computing services could comply with that provision remains a riddle. What's more, the relevant issues of user-generated content and continue to be substantially unaddressed.

Keywords: cloud computing - web 2.0 - right to be forgotten in the EU - right to be forgotten in Italy - *droit à l'oubli* - technical issues in implementing right to erasure - Data Protection Directive - Proposal for a General Data Protection Regulation (GDPR) - art. 17, Court of Justice - Google Spain - evolution of the concept of privacy - privacy by design - balance between fundamental rights and public interest - digital identity - user-generated content.

TABLE OF CONTENTS

SEZIONE I

I. AL CROCEVIA TRA SOCIETÀ INFORMATICA, CLOUD COMPUTING E DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI: LA MAPPA CONCETTUALE PER ORIENTARSI IN UNO SCENARIO COMPLESSO

La tematica del *cloud* riflette il mutamento di paradigma operato in materia di *privacy*: dal diritto alla riservatezza al diritto al controllo e alla protezione dei dati personali, secondo un percorso non sempre lineare alla cui progressione ha contribuito in misura notevole l'affermazione delle tecnologie informatiche[1].

L'ulteriore sviluppo di queste ultime, fino a confluire nel fenomeno in esame, si è caratterizzato per l'accentuazione esasperata dell'elemento dinamico del mondo di *internet*: l'analisi del *cloud computing*, come vedremo nello specifico, incontra il tema dell'interesse individuale alla "autodeterminazione informativa"[2], concetto riassumibile nella possibilità per il soggetto di scegliere, nell'esercizio della propria libera volontà, quali informazioni personali comunicare, nonché i destinatari di queste e le finalità del trattamento.

Per di più, considerandone i vari aspetti tecnici, a ragione si potrebbe sostenere che il *cloud* rappresenta un modello indiscutibile per lo sviluppo del *web* nel suo complesso, fornendo un punto di riferimento per le future evoluzioni di ogni strumento informatico[3].

L'utilizzo del *cloud*, infatti, condensa e attrae a sé una serie di caratteristiche tecnologiche e di fenomeni anche culturali che identificano l'essenza di Internet nella sua espressione attuale, in perfetta coincidenza con l'avvento di quella realtà virtuale implementata riconducibile alla sigla onnicomprensiva di Web 2.0[4].

Rispetto all'era precedente (o, *a posteriori*, Web 1.0), caratterizzata dall'accesso degli utenti a dati prodotti da soggetti terzi o a servizi di semplice ricerca, navigazione e, occasionalmente, *download* (sempre in forme limitate), le innovazioni tecnologiche della rete hanno spostato il fulcro dell'intero sistema sulla nozione di *user-generated content*[5].

---

1 Della sterminata letteratura sul tema, qui rilevante solo in via incidentale, si segnalano G. Resta, *Il diritto alla protezione dei dati personali*, in F. Cardarelli – S. Sica – V. Zeno Zencovich, *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano 2004; anche con un taglio storico S. Rodotà, *Tecnologie e diritti*, Milano 2005, pp. 19-121.

2 Il diritto in questione, sancito per la prima volta dalla Corte Costituzionale tedesca (BVerfG) con sentenza 15 dicembre 1983, 1 BvR 209/83 e fondato sul rispetto del diritto al libero sviluppo della propria personalità e sull'intangibilità della dignità dell'uomo, è stato recentemente arricchito di un ulteriore profilo relativo all'integrità informatica (BVerfG, 27 gennaio 2008, 1 BvR 370/07); la recezione in Italia è avvenuta, ancora vigente la l. 675/1996, fin dalla prima pronuncia del Garante per la protezione dei dati personali, con decisione 25 maggio 1997, in *Corr. giur.*, 1997, 8, p. 915, con nota di V. ZENO ZENCOVICH.

3 Il mutamento più significativo — si sottolinea fin da principio — non risiede nella realizzazione di nuovi strumenti tecnologici, ma nella modalità di impiego delle tecnologie esistenti; d'altra parte, lo stesso carattere "rivoluzionario" del *cloud computing* è spesso sopravvalutato, poiché forme applicative (come le *webmail*) circolano da tempo su Internet. La dimensione innovativa potrebbe cogliersi invece sul piano della generalizzazione di un particolare schema organizzativo-funzionale e della progressiva convergenza su di esso dell'intero ambiente virtuale.

4 Per un'ampia analisi del fenomeno si veda T. O'REILLY, *What is Web 2.0*, 2005, reperibile all'indirizzo *http://oreilly.com/web2/archive/what-is-web-20.html*; l'autore è il padre del termine in questione.

5 Più di carattere tecnico che giuridico gli studi in materia: v. C. E. GEORGE – J. SCERRI, *Web. 2.0 and User-generated Content: Legal Challenges in the New Frontier*, in *Journal of Information, Law, Technology*, 2007, 2, reperibile su SSRN: http://ssrn.com/abstract=1290715; tuttavia, come segnalato oltre, l'inversione di prospettiva si riverbera su aspetti specifici della disciplina applicabile in tema di tutela dei dati personali.

Ogni modalità di configurazione della rete si trasforma infatti in un vero e proprio contenuto, costituendo esercizio di un «potere generativo»[6]: da parte del fornitore, organizzare, aggregare e indicizzare per gli utenti il materiale da essi stessi fornito non può più intendersi come operazione strettamente neutrale, automatica esecuzione delle richieste dei clienti; da parte dell'utente, l'approccio ad Internet esclude ogni atteggiamento passivo, e si misura invece con la diffusione dei comportamenti tendenti a facilitare la personalizzazione dell'interfaccia virtuale e la partecipazione alla produzione e agli scambi di informazioni.

Pertanto, un nodo essenziale del ragionamento è costituito dall'osservazione per cui nella realtà di Internet è venuta decisamente meno la differenza tra fornitore, distributore e fruitore delle informazioni: ciò rappresenta un punto cruciale nell'identificazione dei soggetti in gioco, nella loro qualificazione in termini di categorie giuridiche e, di conseguenza, nella definizione dei diritti e degli obblighi gravanti su ciascuno e dei connessi profili di responsabilità[7].

Il fenomeno sembra così sfuggire ad ogni tipo di limite spaziale o temporale, dal momento che il predominio delle tecnologie dell'informazione e della comunicazione dà luogo ad una scomposizione della soggettività dei singoli individui, ciascuno dei quali non è esaurito dalla realtà fisica, ma estrinseca la propria personalità in una molteplicità di luoghi virtuali, ove si creano diverse identità, relazioni e, di conseguenza, rapporti giuridici[8].

In uno scenario di tal genere, i servizi erogati su Internet sono percepiti come indispensabili e irrinunciabili: una realtà implementata mediante l'impiego di tecnologia *cloud* è connotata da un tasso altissimo di interconnessioni, e la progressiva riduzione della materialità (apparente, almeno) delle informazioni, degli archivi e degli strumenti applicativi, delocalizzati nel *web*, sottolinea gli aspetti di totale affidamento e di dipendenza pratica, nelle operazioni più quotidiane, rispetto ai *server* che conservano i dati.

Come problema collaterale, anche se forse logicamente preliminare, acquista altresì interesse il tema della presenza di infrastrutture adeguate e della loro agibilità ai fini di garantire una connessione effettiva alla rete, in quanto esse costituiscono la porta d'ingresso obbligata nel mondo virtuale: anche sulla base di analisi comparatistiche[9], si discute infatti dell'ammissibilità di un ipotetico "diritto

---

6 Questa la definizione di J. ZITTRAIN, *The generative Internet*, in *Harvard Law Review*, Vol. 119, p. 1974, May 2006. Reperibile su SSRN: http://ssrn.com/abstract=847124.

7 Marcata da una forte attenzione per l'attualità l'analisi, ricca di riferimenti giurisprudenziali, di A. PAPA, *La complessa realtà della Rete tra "creatività" dei fornitori servizi Internet ed esigenze regolatorie pubbliche: la sottile linea di demarcazione tra* provider *di servizi di "*content*" e di "*hosting *attivo"*, in *Economia e diritto del terziario*, 2012, 2, p. 221: il contributo conferma l'idea in base alla quale, per delineare con esattezza l'assetto del rapporto tra fornitore e utente, sono da evitare approcci astratti e deve invece prediligersi un apprezzamento delle circostanze del caso concreto. Notazioni simili, in commento ad un episodio all'origine di numerose riflessioni in dottrina, propongono G. SARTOR – M. V. DE AZEVEDO CUNHA, *Il caso* Google-VidiDown *tra protezione dei dati personali e libertà di espressione* on-line, in *Dir. inf.*, 2010, 4-5, 645. Preme sottolineare fin da subito che tale ragionamento, con pari, se non maggiore, forza persuasiva, può essere esteso a tutti i servizi di *cloud* (*computing*).

8 Sul tema S. SICA – V. ZENO ZENCOVICH, *Legislazione, giurisprudenza e dottrina nel diritto dell'Internet*, in *Diritto dell'informazione e dell'informatica*, 2010, 3, p. 377; più diffusamente S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, II ed., Roma-Bari 2004, pp. 139 ss. Particolarmente apprezzabile il contributo di G. RESTA, *Identità personale e identità digitale*, in *Dir. inf.*, 2007, 3, p. 511, il quale suggerisce due percorsi di lettura del tema dell'identità in rete: da un lato, appunto, l'estensione della dimensione personale giunge fino a coinvolgere l'immaterialità virtuale, la quale, a sua volta, contribuisce a definire i connotati e i tratti distintivi dell'individuo; dall'altro, le informazioni personali concesse dagli utenti vanno a costituire la base per una identificazione (e, aggiungiamo, una profilazione) del soggetto.

9 P. PASSAGLIA, *Diritto di accesso ad Internet e giustizia costituzionale. Una (preliminare) indagine comparata*, in M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet – Atti della tavola rotonda svolta nell'ambito dell'IGF Italia 2010* (Roma, 30 novembre 2010), Napoli, 2011.

all'accesso ad Internet" e della sua copertura costituzionale, in virtù della funzione che esso riveste nell'estrinsecazione delle libertà fondamentali dell'individuo[10].

In termini sia tecnici che sociologici, il *cloud*, soprattutto nella sue forme più versatili e ricche, riassume le caratteristiche predette: a livello di considerazioni di respiro generale, si può dunque affermare — e ne sarà offerta ulteriore dimostrazione empirica — che la struttura di Internet si stia muovendo in linea di convergenza con la realtà integrata costruita sulle fondamenta delle innovazioni riconducibili all'impiego di tecnologia *cloud*, nel senso che alla replicazione degli elementi salienti dell'architettura di quest'ultima sono informati i servizi in rete.

Sul piano che qui interessa più direttamente, delocalizzazione ed ubiquità dei *server*, accessi e flussi continui, conservazione insieme ai dati di innumerevoli altri utenti e utilizzazione contemporanea e condivisa delle risorse (c.d. *resource pooling*)[11], elementi indefettibili di un sistema ad ingegneria *cloud*[12], rappresentano rischi evidenti per la tutela dei dati che inevitabilmente vanno a costituire oggetto del servizio[13].

La questione non risiede soltanto nella tutela della riservatezza assoluta delle informazioni conferite, quanto, in misura socialmente e giuridicamente più rilevante, nell'interesse che le medesime, inevitabilmente coinvolte in attività vantaggiose per l'utente stesso, che ne richiede l'elaborazione, non subiscano trattamenti illegittimi e, in ogni caso, in prospettiva ben distinta, per quanto parallela, forieri di un danno verso il soggetto a cui si riferiscono.

In realtà, il solo fatto che un'informazione esista in rete può essere considerato come un rischio reale ed effettivo, indipendentemente dalla sua collocazione o dal trattamento che ne viene fatto[14]. Ciò tanto più, com'è ovvio, se questi ultimi sono effettuati contro i divieti disposti per legge, ma, alla luce della natura di *internet*, non può ritenersi che il rispetto formale delle regole sia garanzia di tutela effettiva: rimane sempre aperta la possibilità (materiale) che soggetti, sia privati che pubblici, abbiano accesso alle informazioni e le rielaborino per finalità discordi da quelle che ne avevano ispirato il conferimento originario e con modalità non controllate.

Nel modo del *web*, pertanto, assurge a primaria importanza la potenzialità, intesa come reperibilità, e la considerazione è vera soprattutto per il *cloud computing*. Il fenomeno *cloud* in sé, indipendentemente dalla configurazione tecnica di volta in volta assunta, si avvale di un meccanismo che esaspera la dimensione virtuale[15], in cui il servizio (sotto forma vuoi di memorizzazione, vuoi di fornitura di *software*), astrattamente disponibile e non localizzato, si concretizza solo al momento dell'accesso da parte dell'utente e della successiva, conseguente esecuzione della prestazione richiesta. In queste condizioni,

---

10 P. COSTANZO, *Miti e realtà dell'accesso ad Internet* (una prospettiva costituzionalistica), in P. CARETTI (a cura di), *Studi in memoria di Paolo Barile*, Passigli Editore, Firenze 2012; L. NANNIPIERI, *Costituzione e nuove tecnologie: profili costituzionali dell'accesso ad Internet*, relazione al Secondo seminario annuale del "Gruppo di Pisa", Università di Roma Tre, 20 settembre 2013.

11 Autorevole per ufficialità P. MELL – T. GRANCE, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, NIST, January 2011, Special Publications 2.

12 Non pertiene a questa sede chiarire il quadro generale di tale tecnologia, per quanto singoli aspetti rilevanti saranno oggetto di una maggiore accuratezza definitoria in seguito. In ogni caso, per le caratteristiche indicate e per un primo contatto con il tema si può consultare la guida del Garante per la protezione dei dati personali, Cloud computing: *indicazioni per l'utilizzo consapevole dei servizi*, reperibile presso: http://www.garanteprivacy.it/documents/10160/10704/1819933.

13 N. ROBINSON ET AL., *The Cloud: Understanding the security, Privacy and Trust Challenges*, RAND Corporation, 30 novembre 2010, reperibile su SSRN: http://ssrn.com/abstract=2141970.

14 Pregnante la lingua inglese: il dato o l'informazione, comunque dispersa nel *web*, è generalmente considerata *stored*, vale a dire, prima di tutto, non tanto memorizzata o raccolta in apposite infrastrutture organizzate, quanto, semplicemente, "immagazzinata". L'informazione, in ambito virtuale, non appena viene ad esistenza, pur potendo non costituire "notizia" in senso proprio, si impliglia nelle maglie della rete *web*, tramite i cui fili sottili rimane sempre raggiungibile.

15 Contributo improntato al tecnicismo quello di M. A. VOUK, *Cloud computing – Issues, Research and Implementations*, in *Journal of Computing and Information Technology*, 2008, 16, 4, p. 235.

tracciare i dati in ogni momento della loro esistenza incontra non pochi ostacoli, che si riflettono sulle possibilità di regolarne in modo soddisfacente l'impiego e la destinazione.

Le considerazioni latamente tecniche appena svolte, insieme ad altre proposte nel testo che segue, risulteranno assai utili come sistema di riferimento concettuale al momento di andare a trattare i punti salienti della tutela della *privacy* dell'utente apprestata dalla proposta di regolamento generale sul trattamento dei dati[16], allorché si dovranno sondare i margini di coerenza e di applicabilità della introducenda disciplina rispetto alle specificità tecnico-operative del fenomeno del *cloud computing*.

In particolare, non potendo affrontare in modo esaustivo tutte le tematiche lambite nel rapido inquadramento precedente, né, tantomeno, le numerose altre non menzionate[17], pur se attinenti, in via più o meno indiretta, all'ambito della *privacy* in senso lato, l'intervento del legislatore europeo sarà materia di approfondimento del presente lavoro per quanto riguarda lo specifico argomento del c.d. diritto all'oblio, il quale proprio nella bozza del Regolamento riceve la prima codificazione sotto la rubrica di «diritto all'oblio e alla cancellazione»[18]. In campo informatico tale formulazione, alla quale si può essere tentati di ricollegare aprioristiche prese di posizione ideologiche, richiede un'analisi accurata e libera da preconcetti, per accertarne portata, ricadute e limiti applicativi in un ambito, come quello qui delineato, estremamente mutevole e sfuggente, per caratteristiche intrinseche, alla consueta tecnica normativa[19].

II. LA SPECIFICITÀ DEL CLOUD COMPUTING COME PROVA DI RESISTENZA DELLA ATTUALE NOZIONE DI PRIVACY NEL CONFRONTO CON LE ESIGENZE DI CANCELLAZIONE DEI DATI

L'affermazione del fenomeno *cloud* individua il suo nucleo genetico ed essenziale nella messa a disposizione, in remoto, di memoria virtuale e, al contempo, di processori che consentono l'erogazione via Internet di risorse operative e potere elaborativo.

Per soddisfare le esigenze primarie di funzionamento di un sistema *cloud*, quali la memoria e l'accessibilità, l'informazione difficilmente è conservata in copia unica ma, al contrario, di essa esistono più *back-up* i quali, a loro volta, sono archiviati mediante diversi *server* che contribuiscono all'aumento del livello di complessità dell'ecosistema informatico, sia per la loro localizzazione diffusa, sia per i continui flussi di dati che gestiscono e facilitano.

---

16 V. Commissione Europea, *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) 11 final, Bruxelles, 215 gennaio 2012.

17 Prima tra le quali la questione della legge che regola il rapporto, connessa ad una molteplicità di fattori: in questa sede si prescinde dall'ipotesi del conflitto tra leggi, per concentrare l'attenzione sullo studio di una delle possibili leggi (in futuro) applicabili.

18 Così l'art. 17 della proposta di regolamento («*Right to be forgotten and to erasure*» nella versione in lingua inglese).

19 Con un impianto anche filosofico G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Dir. inf.*, 2012, 4-5, p. 831, dove si richiama il concetto di «neutralità tecnologica» e si propugna un approccio del diritto al mondo dell'informatica di tipo "funzionale", auspicando, in prospettiva futura, «la formulazione di regole e di norme attraverso la tecnica»: la soluzione ai problemi relativi alla regolazione di Internet risiederebbe in una *lex informatica* di fonte autonoma, individuabile appunto nei codici e negli altri strumenti tecnologici.

L'aspetto contraddittorio — e che non può non essere considerato ai fini di una migliore comprensione — è che in quasi la totalità dei casi la presenza di un'informazione distribuita sotto forma di copie talvolta numerosissime costituisce un vantaggio pressoché inestimabile non solo e non tanto per il prestatore del servizio, bensì soprattutto per l'utente[20]: l'archiviazione e la dispersione nell'infrastruttura anche fisica del *web* garantiscono due aspetti essenziali delle attività via Internet e dei servizi *cloud*, vale a dire la sicura conservazione e la disponibilità immediata delle informazioni[21].

Tuttavia, al momento della rimozione, ciò può avere effetti negativi, dal momento che per ottenere una cancellazione effettiva dovrebbero essere distrutte tutte le riproduzioni del dato che si intende espungere dalla realtà informatica. Il risultato perfetto, però, è assai difficile da raggiungere: non solo perché appare talvolta irrealistico poter identificare ogni singola copia dell'informazione originaria, soprattutto nel caso di condivisione della stessa con soggetti terzi, ma anche per il motivo forse più rilevante che, al di là dell'informazione in sé, ciò che rimane sono le sue "tracce", stampate in modo indelebile nella memoria della rete. Il dato, infatti, non esiste soltanto come entità sostanziale, ma possiede una dimensione di vita "funzionale" o, meglio, "relazionale": esso risulta definito, oltre che per caratteristiche intrinseche, anche per i rimandi e i collegamenti esterni che ad esso si riferiscono e che lo individuano come ultimo di una serie ordinata di passaggi scanditi da algoritmi e operazioni logico-informatiche[22]. In aggiunta, gli stessi collegamenti possono assumere una fisionomia autonoma e trasformarsi in dato autonomo (come nel caso dell'indicizzazione nei motori di ricerca, a sua volta integrata in altri motori, di dimensioni inferiori o maggiori), con una moltiplicazione potenzialmente indeterminata ed indeterminabile dell'informazione di partenza.

Per questa via, giungiamo a delineare progressivamente la contraddizione cui si accennava prima: il mondo digitale nella versione 2.0 sembra fondare la propria essenza sul dissidio tra esigenza di memoria e, sempre di più, esigenza di cancellazione di dati personali, sottoposti d'altra parte a continue operazioni di diffusione e comunicazione, spesso su base volontaria[23].

---

[20] C. SOGHOIAN, *Caught in the Cloud: privacy, encryption, and Government back doors in the Web 2.0 Era*, in *J. On Telecomm. And High Tech. L.*, 2010, 8, pp. 365-366.

[21] Questi alcuni tra i principali obblighi del prestatore in base ai c.d. *service agreements*: L. BADGER ET AL., *Cloud computing synopsis and recommendations*, NIST, *Special Publication* 800-146, May 2012, par. 3.1.

[22] Il punto può offrire l'occasione per discutere se Internet sia organizzato in modo da costituire un vero e proprio archivio: risponde negativamente G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. inf.*, 2010, 3, pp. 392-394, per la quale «la memoria della Rete […] assomiglia molto di più ad un deposito, nel quale ci sono degli archivi» e in cui i motori di ricerca svolgono un ruolo fondamentale nel determinare le informazioni accessibili. Il tema sarà riproposto più avanti.

[23] Spunti in G. FINOCCHIARO, *La memoria della rete*, cit., pp. 395 ss.; di notevole interesse e di pregevole fattura per chiarezza e ricostruzione storica V. MAYER–SCHÖNBERGER, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009.

II. 1. UNA TAPPA DI AVVICINAMENTO: PROBLEMI E SOLUZIONI NEL MODELLO *IAAS*

Con particolare attenzione ai servizi di tipo *cloud*, conviene considerare innanzitutto i più semplici casi di *IaaS* (*Infrastructure as a Service*), in cui il servizio reso costituisce il mero supporto ad un'attività di memorizzazione di dati personali di cui è immediato individuare le ragioni nella delega di una funzione di conservazione di materiale privato in base a considerazioni di opportunità, praticità e sicurezza[24]: in altre parole, quello che si potrebbe archiviare sul proprio terminale è depositato in un altrove virtuale, con i connessi vantaggi in termini di riduzione del rischio di perdita, totale o parziale, e di incremento dell'accessibilità.

L'utente, con un atteggiamento coerente che consideri l'infrastruttura messa a disposizione dal *provider* come nient'altro che una propaggine del proprio spazio privato, fatta salva la possibilità di falle nel sistema informatico, ben potrà appellarsi alla nozione più tradizionale (e storicamente, per così dire, primordiale) di *privacy* e dunque potrà far valere il proprio diritto alla riservatezza, ossia legittimamente opporsi ad indebite intrusioni nella propria sfera privata.

Se, infatti, com'è auspicabile, il sistema fornito dal *provider* presenta un adeguato livello di misure tecniche di sicurezza[25] e il servizio assume connotati prevalentemente statici, non si pone neppure il problema di una fuga di notizie o di una loro incorporazione o integrazione in altre banche dati[26]: la questione di un eventuale diritto alla cancellazione si risolve nella facoltà per l'utente — già riconosciuta e comunque facilmente concepibile nell'ambito della disciplina convenzionale del servizio o della singola prestazione[27] — di chiedere l'eliminazione della singola informazione e di ogni sua copia conservata presso i *server* del fornitore, di rimuoverla personalmente nonché di ottenerne la distruzione completa al momento in cui termina il servizio.

---

[24] Cfr. E. PROSPERETTI, *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema* cloud, in G. CASSANO – G. VACIAGO – G. SCORZA (a cura di), *Diritto dell'Internet. Manuale operativo: casi, legislazione, giurisprudenza*, Cedam, 2012, p. 679.

[25] Questo è garantito dal c.d. SLA (*Service Level Agreement*), un documento vincolante le parti spesso allegato al contratto in cui si stabiliscono «*the technical performance promises made by a provider including remedies for performance failures*»: cfr. L. BADGER ET AL., *Cloud computing*, loc. cit.

[26] In questo senso rileva, nell'ambito della proposta di regolamento, l'art. 30, par. 2, il quale, con un'estensione dei soggetti destinatari dell'obbligo (in precedenza diretto al solo responsabile del trattamento, v. art. 17, par. 1, dir. 95/46), recita: «Previa valutazione dei rischi, il responsabile del trattamento e l'incaricato del trattamento prendono le misure [tecniche e organizzative adeguate] per impedire qualsiasi forma illegittima di trattamento, in particolare la comunicazione, la divulgazione o l'accesso non autorizzati o la modifica dei dati personali».

[27] Sulle "condizioni del servizio", comunque denominate, interessante e vario il contributo di P. SAMMARCO, *Le clausole contrattuali di esonero e trasferimento della responsabilità inserite nei termini d'uso dei servizi del* Web *2.0*, in *Dir. inf.*, 2010, 4-5, pp. 632 ss. Vero è, peraltro, che la fonte primaria di regolamentazione dei rapporti tra utenti e *provider* consiste nella posizione di controllo e gestione unilaterale dell'infrastruttura da quest'ultimo detenuta: ulteriori riflessioni sulle regole di utilizzo di servizi informatici quali i *social network* (partecipi di numerosi aspetti del *cloud computing*) in S. SCALZINI, *I servizi di* online social network *tra* privacy*, regole di utilizzo e violazioni dei diritti dei terzi*, in *Giur. merito*, 2012, 12, pp. 2573 ss., dove si fa pure riferimento all'autorevole contributo sul tema della governance della rete di L. LESSIG, *Code Version 2.0*, pp. 200 ss., reperibile presso l'indirizzo http://codev2.cc/download+remix/Lessig-Codev2.pdf.

Nonostante alcune incertezze sui tempi di cancellazione[28], si verifica quindi la circostanza per cui, a patto che siano rispettate le clausole stipulate, i dati conferiti dall'utente saranno oggetto del solo rapporto tra quest'ultimo e il fornitore del servizio: se ciò non vale ad escludere in radice il problema di una interferenza nella sfera delle informazioni personali del singolo, in quanto il compito di prendersene cura è inevitabilmente delegato ad "esterni", che pure lo esercitano in qualità di professionisti, sono ridotte al minimo le occasioni in cui soggetti ulteriori, indeterminati o indeterminabili, possono inserirsi e provocare la rottura del delicato equilibrio tra attività di memorizzazione (garantite dall'infrastruttura *cloud*) e attività di cancellazione (materialmente possibili fin quando i dati sono controllati e tracciabili).

Non vi è dunque contraddizione: come visto, è plausibile, con le dovute precauzioni, che le prime siano svolte in modo efficace e, allo stesso tempo, senza pregiudicare un futuro esercizio delle seconde.

Si ribadisce, sia pure in via incidentale, che da ciò dovrebbe trarsi spunto per riflettere sul ruolo assunto dai soggetti in gioco, e dunque sulla qualificazione di questi in base alla disciplina sul trattamento dei dati personali[29]: definire *controller* e *processor*, passaggio fondamentale per chiarire le posizioni di utente e fornitore sul piano giuridico, nonché le modalità in cui gli interessati possono esercitare i propri diritti, implica tuttavia un'analisi che esula, non per pertinenza, ma per complessità, dalla presente trattazione, la quale tuttavia, di necessità, dovrà in alcune occasioni farvi ricorso.

Proseguendo con il ragionamento, si può notare come l'assunto di partenza sia lineare e quasi scolastico: pur senza tenere in considerazione eventuali comportamenti scorretti e addirittura illeciti del *provider* (il quale, ad esempio, continua comunque a detenere una copia dei dati anche in un momento successivo alla richiesta fondata di cancellazione o alla terminazione del servizio, per finalità tra le più disparate), è improbabile, per la natura intrinseca delle attività informatiche e ancor più per le ragioni stesse che spingono le imprese ad investire in Internet, che il servizio sia limitato al semplice gruppo di operazioni sopra delineato e che al momento dell'accettazione delle condizioni generali (c.d. *Terms and Conditions*) e della conclusione del contratto non sia prestato il consenso al compimento, da parte del fornitore, di una serie di azioni concernenti i dati aliene alla semplice memorizzazione[30] ovvero

[28] Anche per questi tipi di servizi si tenga presente lo studio casistico in S. BRADSHAW – C. MILLARD – I. WALDEN, *Contracts for Cloud: Comparison and Analysis of the term and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper 63/2010, pp. 23 ss.

[29] E. PROSPERETTI, *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema* cloud, cit., p. 684.

[30] Si vedano quale esempio le "Norme sulla *privacy*" del servizio *Dropbox* (classico esempio di *IaaS*): alla voce "Come utilizziamo le informazioni personali" si esplicita che queste «vengono utilizzate o possono essere utilizzate per (i) fornire e migliorare il nostro servizio, (ii) amministrare l'uso del servizio da parte dell'utente, (iii) comprendere meglio le esigenze e gli interessi dell'utente dell'utente, (iv) personalizzare e migliorare l'esperienza dell'utente e (v) fornire oppure offrire aggiornamenti software o annunci relativi a prodotti». È evidente come il carattere generico di tali finalità possa giustificare una vastissima gamma di trattamenti non specificati.

accomunate dalla caratteristica di rendere le informazioni personali conferiti accessibili a terzi, sotto le forme e nelle modalità più varie[31].

In queste circostanze, dunque, l'esigenza di approntare una tutela effettiva impone di spostare l'attenzione, come già poteva immaginarsi, al momento della conclusione del contratto atipico di fornitura del servizio. Le condizioni d'uso dovrebbero essere corredate di una specifica informativa della *privacy* così che i dati conferiti non siano sottoposti ad operazioni impreviste, alle quali mai l'utente avrebbe prestato il consenso o che implicherebbero la conclusione di un diverso contratto[32]: vengono in rilievo soprattutto le informazioni relative a «le finalità del trattamento cui sono destinati i dati personali, compresi i termini contrattuali e le condizioni generali […]», «il periodo per il quale i dati sono conservati» e «i destinatari o le categorie di destinatari dei dati personali» (art. 14, par. 1, lett. b), c) e f), della proposta di regolamento)[33].

II.2. PAAS E SAAS TRA NECESSITÀ DI MEMORIA E RICHIESTE DI CANCELLAZIONE: CRONACA DI UN DISSIDIO ANNUNCIATO

Il quadro perde ulteriormente di nitidezza nel momento in cui si abbandona lo scenario in cui l'utente, in un ambito esclusivamente privato, in funzione di mera ausiliarietà e senza alcuna attribuzione di compiti attivi al *provider*, utilizza il servizio come deposito di contenuti di varia natura connotato da una spiccata passività: la preponderante conformazione assunta dal servizio in oggetto è invece quella di *cloud computing*, di cui si distinguono solitamente due modelli, *SaaS* e *PaaS*.

Entrambi questi ultimi segnano il definitivo abbandono del paradigma che prevedeva un controllo fisico dell'utente sui propri dati, *file* e, in generale, risorse informatiche, i quali adesso, con notevoli vantaggi connessi alla riduzione dei rischi di distruzione o perdita e di esaurimento della capacità di memoria dei calcolatori, sono conservati presso *server* delocalizzati gestiti da imprese private[34]: il mutamento più significativo non si è realizzato con la semplice possibilità di archiviare contenuti su

31 Sempre le Condizioni d'uso di *Dropbox* prevedono, alla voce "Condivisione e divulgazione delle informazioni": «Possiamo utilizzare alcune imprese e alcuni terzi affidabili per aiutarci a fornire, analizzare e migliorare il Servizio […]. Tali parti terze possono avere accesso alle informazioni dell'utente per poter svolgere queste attività». È comunque previsto che tale accesso avvenga nel rispetto delle "Norme sulla *privacy*" interne e che, in ogni caso, la condivisione delle informazioni con un'applicazione di terze parti sia subordinata al consenso dell'utente.

32 Vale infatti l'osservazione per cui «dal punto di vista giuridico, il concreto assetto del rapporto contrattuale che presiede ad un rapporto di *cloud* dipende […] dall'effettivo oggetto e contenuto della prestazione che viene richiesta dal cliente al *cloud provider*»: E. PROSPERETTI, *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema* cloud, cit., p. 680.

33 Si potrebbe essere tentati di suggerire l'applicazione di un così semplice strumento anche alle forme di *cloud* di cui si dirà immediatamente a seguire: in tali ipotesi, tuttavia, come sarà opportunamente dimostrato, attesa la particolare configurazione del servizio, anche in ragione delle necessità degli utenti del medesimo, la comunicazione preliminare delle modalità del trattamento dei dati non può che rivestire, per forza di cose, un'efficacia quantomeno dimidiata e comunque, sebbene contribuisca al procedimento di corretta integrazione degli elementi essenziali del consenso informato, per la sua caratteristica di salvaguardia minima è destinata ad operare solo in una fase limitata della vita digitale delle informazioni.

34 C. SOGHOIAN, *Caught in the Cloud*, cit., pp. 362-364.

Internet (in un procedimento scomponibile nelle due fasi di necessario "caricamento" o *upload* e di successivo *download* secondo le necessità del caso)[35], bensì con la migrazione in rete di applicazioni di ogni genere e la nascita di servizi appositi che ne permettono una diretta fruizione.

La distinzione tra i modelli richiamati, appartenenti alla categoria appena indicata, e dunque contraddistinti dalla sostituzione delle attività che l'utente svolgerebbe normalmente sul proprio terminale con l'erogazione in modalità *online* di servizi equivalenti, può apparire al profano piuttosto sottile. Nell'impossibilità di offrire dettagli tecnici completi[36], una sintesi efficace evidenzia comunque che, una volta colta la differenza rispetto alla tipologia *IaaS*, nelle ipotesi di *PaaS* (*Platform as a Service*) il servizio è rivolto soprattutto all'offerta di risorse per lo sviluppo di ulteriori applicazioni o soluzioni operative proprie, eventualmente anche da fornire a terzi; a sua volta, lo schema *SaaS* (*Software as a Service*), rendendo possibile all'utente di utilizzare un sistema versatile e personalizzabile per muoversi nell'ambito di un complesso ambiente *web*, risulta costruito sui modelli precedenti, di cui necessariamente eredita gli aspetti problematici in termini di gestione dei dati (localizzazione, memorizzazione ed accesso) e sicurezza della rete.

L'esternalizzazione delle informazioni — tratto comune al modello *IaaS* — nel caso di utilizzo di applicazioni in linea implica nuove sfide di carattere tecnico sul piano della sicurezza delle informazioni[37] e risulta fonte di maggiori preoccupazioni in materia di *privacy*.

Da un lato, infatti, i dati coinvolti possono essere più numerosi, sia per la natura intrinseca del servizio, attraverso il quale l'utente svolge una serie di attività quotidiane, rivelatrici delle proprie abitudini e caratteristiche, attinenti alla propria sfera privata (per questi aspetti, si pensi alle *webmail*) o ancora di estrinsecazione della propria personalità (calzante l'esempio dei *social network*), sia per la maggiore diffusione di tale tipologia di *cloud*, più versatile e idonea a soddisfare esigenze di vario genere.

Dall'altro lato, le applicazioni stesse, in quanto proiettate in una dimensione dinamica, sottopongono i dati a continue elaborazioni e possono richiedere, per un funzionamento efficace, maggiori interazioni con altre informazioni o la condivisione di quelle già detenute con soggetti terzi, sviluppatori o prestatori di servizi ausiliari[38].

---

35 Schema corrispondente ai servizi *cloud* denominati *IaaS*.

36 Per le considerazioni immediatamente seguenti, comunque, il riferimento è l'approfondito K. HASHIZUME ET AL., *An analysis of security issues for cloud computing*, in *Journal of Internet Services and Application*, 2013, 4.

37 Si veda ancora la puntuale analisi di L. BADGER ET AL., *Cloud computing*, parr. 5.4 (per il *SaaS*) e 6.4 (per il *PaaS*).

38 Si tratterebbe di veri e propri subcontraenti, i quali poi assumono il ruolo, nell'ambito della disciplina sul trattamento dei dati personali, di subincaricati, con precise ricadute in termini di obblighi giuridici: si veda ART. 29 WP, *Parere 5/2012 sul* cloud computing, WP196, adottato il 1° luglio 2012, par. 3.3.2. A causa della recente esplosione del fenomeno, determinata in primo luogo dalla diffusione di dispositivi portatili connessi in modo continuo alla rete Internet (*smartphone* e *tablet*), l'attenzione si va concentrando sulle "applicazioni" o *app*, servizi offerti da soggetti diversi dal gestore della piattaforma operativa principale: in proposito si segnala la *Warsaw declaration on the "appification" of society,* adottata il 24 settembre 2013 in seno alla 35ª Conferenza internazionale dei responsabili delle autorità garanti per la protezione dei dati personali e la *privacy*.

L'utente cede una parte importante del controllo sui propri dati in modo progressivo a seconda dei modelli considerati: se il modello *IaaS*, come visto, può essere ricondotto alla mera fornitura di una capacità di memorizzazione e di spazio disco esterna, il cui utilizzo è lasciato all'arbitrio di chi ne fruisce, in ipotesi di *PaaS* e *SaaS* l'alto livello di integrazione dei servizi offerti, l'ampia gamma di fonti di conferimento delle informazioni e la complessità (in senso oggettivo e soggettivo) della catena di esternalizzazione determinano una perdita di contatto con i dati a svantaggio del soggetto cui si riferiscono e l'incremento del rischio per i clienti «di non poter prendere le misure tecniche e organizzative necessarie per garantire la disponibilità, l'integrità, la riservatezza, la trasparenza, l'isolamento, la portabilità dei dati e la possibilità di intervento sugli stessi»[39].

Anche se accennate, la caratteristiche degli ultimi due modelli sono estremamente rilevanti quando si esamini il residuare di possibilità di effettiva cancellazione dei dati conferiti e di quelli al cui trattamento si è acconsentito ai fini dell'utilizzo del sistema *cloud*, con le ricadute da vedersi per quanto concerne l'applicazione della proposta di regolamento in materia di "diritto all'oblio".

Alla luce delle riflessioni svolte, infatti, la configurazione di *PaaS* e *SaaS* impedisce di condividere la visione riduzionista e generica sintetizzata dalle parole «*if an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system*»[40]. Questa espressione (di chiaro contenuto "politico"), per quanto corretta nell'equilibrio dei fattori considerati, pare ignorare il concetto generale che si tenta di far emergere, in base al quale la revoca del consenso originariamente prestato non può comunque assumere forza tale da cancellare (tutti) gli effetti interinali prodottisi nella realtà, virtuale e non, soprattutto nell'ambito del *cloud computing*.

Esclusi appunto i casi di *IaaS* — per i quali, a livello astratto, è già individuabile una tutela specifica e che, comunque, rientrano in un quadro meno confuso — almeno tre rilievi si segnalano con particolare evidenza: le considerazioni seguenti, sebbene svolte su dichiarazioni prive di valore normativo, tuttavia possono sottolineare alcuni inconvenienti concettuali connessi ad un approccio aprioristico al fenomeno.

I primi due aspetti sono sintomatici delle problematiche connesse alla dispersione delle informazioni una volta che siano state immesse sulla rete, nella quale sono destinate a rimanere intrappolate, sottratte

[39] ART. 29 WP, *Parere 5/2012*, cit., par. 2.

[40] V. READING (Vice-presidente della Comissione europea), *The EU Data Protection Reform 2012: making Europe the Standard Setter for Modern Data Protection Rules*, 22 gennaio 2012; formulazione pressoché identica è contenuta nei due opuscoli della Commissione *Perché è necessaria una riforma della protezione dei dati nell'Unione europea?* e *In che modo la riforma della protezione dei dati rafforza i diritti dei cittadini?* (accesso ad entrambi tramite http://ec.europa.eu/justice/data-protection/index_it.htm) in risposta alla domanda «Quali saranno i principali cambiamenti?».

ad ogni controllo dell'interessato tramite il quale sarebbero rintracciabili ed eliminabili nelle specifiche ipotesi previste[41].

Innanzitutto, per la natura dei servizi considerati, un ostacolo preliminare è costituito dalla difficoltà di individuare il soggetto definibile come *controller*, tanto dal punto di vista della qualificazione giuridica, quanto della concreta identificazione tra una miriade di possibili soggetti che, a diverso titolo, siano venuti a contatto con i dati[42].

In secondo luogo, la rimozione dei dati dal sistema informatico ad opera del *controller* garantisce in modo solo parziale e insufficiente la riservatezza dell'interessato, poiché è spesso impossibile verificare la presenza di ulteriori copie delle informazioni presso *server* controllati da terzi, le quali non potrebbero essere localizzate o raggiunte, né tantomeno cancellate[43].

In terzo luogo, deve darsi rilievo alla possibilità che il soggetto a cui i dati si riferiscono abbia un interesse a che quegli stessi dati siano conosciuti pubblicamente e che questa sia una delle ragioni principali per le quali usufruisce del sistema *cloud*. Il punto è particolarmente rilevante e merita una spiegazione specifica, in quanto consente di cogliere l'essenza degli interessi sottostanti all'agire dei diversi soggetti, in particolare per ciò che riguarda l'utente finale: quest'ultimo è consapevole delle opportunità offerte dalla rete e rivolge la propria attenzione a quei servizi che mettono in comunicazione utenti e ne agevolano, tramite tecnologie da esse sviluppate o gestite, la condivisione di contenuti.

Il fenomeno, per quanto non esaurisca la totalità degli impieghi del *cloud computing*, assume una spiccata rilevanza, potendo corrispondere a interessi anche non direttamente patrimoniali dell'interessato: le tecnologie informatiche in esame hanno natura neutrale e, pertanto, un'applicazione trasversale, poiché destinate tanto ad imprenditori e professionisti, che attraverso queste perseguono finalità di pubblicità della propria attività o commercializzazione dei propri prodotti, quanto a quegli individui che vi ricercano un modo di organizzare, gestire e promuovere la vita di relazione con altri singoli o gruppi sociali.

Deve peraltro presumersi che tutti i soggetti richiamati accettino anche implicitamente di cedere parte del controllo sui propri dati e, parallelamente, di assumersi i rischi in fatto di *privacy* che ciò comporta, in

---

41 Nodo concettuale ampiamente sviluppato da F. PIZZETTI, *Il prisma del diritto all'oblio*, in IDEM, *Il caso del diritto all'oblio*, Giappichelli, 2013, pp. 37 ss.

42 Fonte di problemi estremamente complessi è la identificazione del responsabile del trattamento prevalentemente con l'utente del servizio: sebbene questa sia la tesi sposata e ribadita più volte in ART. 29 WP, *Parere 5/2012*, cit., spec. par. 3.3, lo stesso Gruppo di lavoro, al par. 3.3.1, riconosce che «si possono presentare situazioni in cui un fornitore di servizi *cloud* può essere considerato corresponsabile o responsabile a pieno titolo, a seconda delle circostanze concrete». Nonostante l'affermazione assuma, nel quadro tracciato nel documento cui si fa riferimento, una rilevanza quasi marginale, una lettura della condizioni d'uso e della realtà operativa del servizio potrebbe indurre a propendere per questa soluzione in un numero di ipotesi decisamente maggiore a quanto prospettato.

43 Allo stesso tempo il problema è aggravato dal fenomeno di "avvicinamento" degli utenti mediante i motori di ricerca alla congerie di informazioni dispersa su Internet, le quali possono emergere in casi e modalità del tutto imprevedibili ed entrare in contatto con soggetti non indentificabili: cfr. G. D'ACQUISTO, *Diritto all'oblio: tra tecnologia e diritto*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, cit., p. 105.

cambio di una gestione più efficace ai fini di volta in volta promossi dal *provider*, siano essi la fornitura di un portale di posta elettronica integrato con rubriche e calendari ovvero di un servizio di *social networking* rivolto alla condivisione pubblica di alcune informazioni in continuo aggiornamento. Per ottenere gli innumerevoli vantaggi offerti dai modelli di *cloud* è impensabile negare l'accesso del prestatore del servizio alle informazioni di volta in volta rilevanti, e dunque l'utente non può che acconsentire, soprattutto quando egli stesso richiede che il prodotto fornitogli si distingua in positivo per capacità di diffondere in modo mirato i dati conferiti[44].

In queste circostanze si realizza con chiarezza il paradosso cui si è fatto riferimento, e i due poli della memoria e della cancellazione giungono al massimo attrito: se è pur vero che il soggetto, nel momento in cui richiede la cancellazione di un dato, nega per definizione l'esigenza di archiviazione dello stesso, non si può non tenere conto di due aspetti cruciali.

Non è insensato, infatti, ritenere che in capo all'individuo permanga, per quanto detto prima, almeno in via astratta e a livello generale, il medesimo interesse alla circolazione di informazioni che ha determinato la fruizione originaria del servizio: a riprova di ciò, da un lato, è probabile che la richiesta di cancellazione sia rivolta a specifici contenuti o singoli dati, dall'altro, la volontà di eliminare un'informazione considerata potenzialmente dannosa per l'immagine personale rivela proprio l'intenzione di mantenere questa in buona luce agli occhi del pubblico (ossia, prima di tutto, della comunità dei fruitori del servizio) e, dunque, come logica conseguenza, di non rinunciare drasticamente a mostrare la stessa, auto-imponendosi una sorta di isolamento informatico.

Anche la memoria, quindi, conserva un proprio valore e sembra prevalere nel confronto con la cancellazione, almeno con riferimento all'identità digitale nel suo complesso o alla generalità dei dati riguardanti un soggetto; per quanto riguarda il singolo dato, invece, nonostante sia avvertita come superiore l'esigenza di eliminare l'informazione, è quasi inevitabile — ed è questo il secondo aspetto che non può essere trascurato — scontrarsi con una realtà in cui la rimozione totale da Internet non è materialmente possibile.

Merita attenzione una nota conclusiva: come si accennava, considerazioni parzialmente analoghe, almeno per quanto concerne gli effetti della fruizione del servizio sull'ambito operativo del diritto alla cancellazione, possono svolgersi anche per quanto riguarda il modello *IaaS*. A ben guardare, infatti, la prospettiva semplicistica è verosimilmente da abbandonare già nel caso di semplice deposito virtuale dell'informazione: vuoi perché il *provider*, per quanto all'apparenza neutrale rispetto al contenuto fornito dall'utente, consente l'accesso a terzi, eventualmente stabiliti in Stati in cui non risulta applicabile la

[44] Alla luce di queste riflessioni sorgono dubbi spontanei intorno alla libertà del consenso prestato: questa appare in pericolo ogni qual volta il servizio cui si desidera accedere richieda come presupposto operazionale, talora persino come materia prima dell'intera funzionalità, il conferimento di dati personali, a maggior ragione se questo ha assunto un rilievo primario nella costruzione di aspetti ineludibili della vita quotidiana o nell'esercizio di diritti della personalità.

disciplina europea, ovvero trasmette a questi una parte o la totalità dei dati o delle elaborazioni statistiche dei dati[45], vuoi perché il medesimo non si limita a conservare i dati, ma ne determina e ne propone all'utente anche solo una speciale configurazione organizzativa[46].

Si ricade evidentemente, seppure in via attenuata, nelle ipotesi di *cloud computing* più diffuse, con una differenza: è probabile che il particolare regime cui sono assoggettati i dati sia l'effetto scaturente da una sapiente arte contrattuale da parte del fornitore[47], piuttosto che dall'accettazione implicita e cosciente dei rischi della società dell'informazione da parte dell'utente, il quale, al contrario, forse ignorava i reali termini e condizioni del servizio, quantomeno nella parte in cui si prevede la messa a disposizione di terzi o, in generale, l'impiego a fini commerciali, estranei ai suoi intenti[48]. Con maggiore chiarezza: da un lato, l'utilizzo di tecnologia *cloud* sotto forma di *SaaS* e *PaaS* presuppone, dalla parte di chi ne fruisce, come visto, la consapevolezza di un qualche compromesso e di una ponderazione (si direbbe un *trade off)* tra la rinuncia ad una sicurezza assoluta in fatto di tutela dei dati personali e i vantaggi che potrebbero derivare sul piano della visibilità e dell'interazione con altri soggetti a fini economici o socio-culturali[49]; dall'altro, invece, nell'ipotesi di *Iaas*, il soggetto a cui i dati si riferiscono è alla ricerca di una particolare prestazione a cui egli non tende ad associare plausibili prospettive di rischio per la *privacy*, a causa della portata circoscritta delle attività a cui suppone i suoi dati siano sottoposti dal fornitore in ragione della presunta essenzialità del servizio[50].

---

45 È evidente come tale situazione si mostri idonea ad azionare il meccanismo di responsabilità, da inadempimento o da fatto illecito, del prestatore nei confronti dell'utente. Tuttavia, è altrettanto agile considerare come, nella prospettiva di studio qui adottata, un approccio coerente alla natura dell'interesse sotteso al diritto alla *privacy* e, in prospettiva, al diritto all'oblio, impone di compiere una valutazione attinente ad una dimensione preliminare rispetto al verificarsi della lesione: ciò non tanto a causa dell'inadeguatezza delle funzioni proprie dell'istituto risarcitorio in simili contesti (profilo meritevole di uno studio apposito e relativo ad un problema separato), quanto in ragione dell'obiettivo di individuare profili di rischio e, di conseguenza, strumenti di cautela tali da incidere in via preventiva e cautelare sul pericolo di una diffusione incontrollata dei dati.

46 Quest'ultimo tema si ricollega a quei fenomeni che hanno determinato l'emersione giurisprudenziale della figura soggettiva atipica dell'*Internet Service Provider* qualificabile come "*host* attivo", spesso utilizzato con riferimento ai c.d. intermediari tecnici di rete: oltre al noto caso *Google-ViviDown*, cui si è fatto riferimento in precedenza (e rispetto al quale deve menzionarsi l'ulteriore riflessione sviluppata in sede di giudizio di secondo grado dalla Corte d'Appello di Milano, 27 febbraio 2013, in *Corr. merito*, 7, p. 766, con nota di A. INGRASSIA), si vedano, più recenti, Trib. Milano, 31 marzo 2011 e Trib. Roma, 11 luglio 2011, entrambi con nota di E. TOSI, *La responsabilità civile per fatto illecito degli* ISP *e dei motori di ricerca*, in *Riv. dir. ind.*, 2012, 1, p. 44; v. ancora A. PAPA, *La complessa realtà della rete*, cit., pp. 248-251.

47 Per considerazioni più ampie sul tema si consiglia A. COGO, *Le regole del contratto tra* social network *e utente sull'uso della proprietà intellettuale del festore, dell'utente e degli altri utenti — riflessioni a partire dall'individuazione del fenomeno, dei suoi soggetti e della funzione del contratto*, in *Annali Italiani del diritto d'autore, della cultura e dello spettacolo* (*AIDA*), XX, 2011, pp. 312-313.

48 Come si è potuto rilevare attraverso studi empirici, per l'utente si dimostra sufficiente una sensazione di controllo, derivante dalla possibilità di regolare la fase di pubblicazione, a fronte della quale egli mostra una maggiore propensione alla condivisione di informazioni e dati personali, indipendentemente dai reali parametri di sicurezza oggettiva, i quali possono addirittura peggiorare: L. BRANDIMARTE – A. ACQUISTI – G. LOEWENSTEIN, *Misplaced Confidences: Privacy and the Control Paradox*, reperibile all'indirizzo http://www.futureofprivacy.org/wp-content/uploads/2010/07/Misplaced-Confidences-acquisti-FPF.pdf .

49 A tale proposito viene in rilievo il limite stabilito, ai fini di una tutela efficace dell'interessato, in ART. 29 WP, *Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, adottato il 16 febbraio 2010, par. III.2: «lo squilibrio fra il potere contrattuale di un piccolo responsabile del trattamento rispetto a un grosso fornitore di servizi non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati».

50 V. ART. 29 WP, *Parere 5/2012*, cit., par. 2, laddove si osserva che «[l]a disponibilità di informazioni insufficienti sulle operazioni di trattamento nei servizi *cloud* rappresenta un rischio per i responsabili del trattamento e per gli interessati, che potrebbero non essere consapevoli di potenziali rischi e minacce e pertanto non prendere misure appropriate».

Quindi, teoricamente, la situazione sarebbe più delicata: potrebbe però individuarsi una soluzione agendo sugli obblighi di informazione (come segnalato in precedenza)[51] e in generale sui limiti anche tecnici e sui doveri imposti al *provider*[52], per quali è auspicabile un'applicazione estensiva, tale da comprendere anche i modelli *PaaS* e *SaaS*.

In definitiva, lo stesso interesse alla memoria (profilo della conservazione e dell'accessibilità presente anche nei modelli *IaaS*) e alla diffusione dell'informazione (profilo dinamico dei modelli *SaaS* e *PaaS*) che anima la scelta del servizio di *cloud computing* si rivela operare *de facto* quasi come una preclusione assoluta all'esperimento di pur giustificate e normalmente prevedibili esigenze di cancellazione, più o meno selettiva, dei dati conferiti. Cosa significhi cancellare i dati in questi casi, quando ciò sia giuridicamente possibile, quali siano le garanzie riconosciute all'interessato e se esistano alternative alla rimozione saranno gli interrogativi lungo i quali si snoderà il prosieguo della trattazione.

SEZIONE II

REALTÀ, INTERPRETAZIONE, RIFORMA E FUTURO DEL C.D. DIRITTO ALL'OBLIO A LIVELLO DELL'UE

III. QUALE «RIGHT TO BE FORGOTTEN» OGGI IN EUROPA? UNA RECENTE LETTURA DEI (RETICENTI) FRAMMENTI NORMATIVI DI ORIGINE COMUNITARIA

Un caso recente consente di gettare luce sulla materia offrendo la possibilità di valutare in chiave comparativa rispetto alla proposta di regolamento la latitudine della tutela apprestata dalla disciplina originaria, attualmente vigente[53], alle ipotesi delle quali si discute, accomunate, in via generale[54], dalla pretesa di un soggetto di ottenere la cancellazione di sue informazioni personali disseminate nel *web*.

I fatti suscitano interesse anche per il coinvolgimento di un motore di ricerca, vale a dire di un soggetto la cui natura e la cui qualificazione, tutt'ora lungi dall'essere compresa e comunque dibattuta, anche a

[51] I quali, tuttalpiù, nei casi in cui emergessero forme di trattamento ulteriori rispetto alla semplice memorizzazione, ricondurrebbero nei fatti alle ipotesi di *PaaS* e *SaaS*.
[52] Sugli obblighi in capo al *cloud provider* di preservare la riservatezza, l'integrità e la disponibilità dei dati si veda E. PROSPERETTI, *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema* cloud, cit., pp. 688-689.
[53] 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, in *OJ* L281, 23.11.95, pp. 31-50; l'Italia ha dato attuazione alla direttiva con la l. 31 dicembre 1996, n. 675, recante norme a tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, poi abrogata e sostituita dal d. lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali.
[54] Lo scenario guadagnerà di precisione e, auspicabilmente, completezza e sistematicità nel prosieguo della trattazione.

livello internazionale[55], non poteva non risultare sfuggente ad un legislatore comunitario ancora inesperto, per necessità, di protezione della dimensione digitale della persona. Al momento dell'approvazione della direttiva 95/46 Internet stesso appariva come fenomeno sconosciuto e certo era impossibile prevedere lo sviluppo futuro dei motori di ricerca: con l'evoluzione della realtà informatica, però, l'importanza di questi ultimi è divenuta innegabile, in quanto il raggiungimento di informazioni di ogni genere, anche se ormai dimenticate, è realizzato attraverso collegamenti dagli stessi forniti, i quali, in tale prospettiva, da un lato determinano in larga misura l'effetto di "eterna memoria" tipico della rete, dall'altro costituiscono, per contenuto, struttura e possibilità di sfruttamento economico, insiemi autonomi di dati, fortemente caratterizzati per organizzazione e pubblicità.

Un sunto[56] della vicenda cui si fa riferimento rafforza il valore dell'esempio: un giornale spagnolo di ampia diffusione aveva pubblicato in edizione cartacea annunci i quali menzionavano un proprietario di immobili come soggetto a procedimento esecutivo. Dopo alcuni anni, la persona interessata, appresa l'esistenza di una versione elettronica del giornale contenente l'annuncio, dopo aver inutilmente richiesto all'editore di rimuovere l'informazione, ha presentato reclamo all'Autorità spagnola per la protezione dei dati (AEPD) contro l'editore stesso e *Google*. La domanda diretta nei confronti di quest'ultimo chiedeva la cancellazione dei dati del soggetto in modo tale che, al momento dell'inserimento nel motore di ricerca del nome e del cognome dell'interessato, non comparisse tra i risultati un collegamento all'articolo contenente l'annuncio.

Il Tribunale di Madrid (*Audiencia Nacionale*), in sede di impugnazione promossa da *Google* contro la decisione che accoglieva il reclamo e ingiungeva di ritirare i dati dall'indice dei risultati e di impedire ulteriori accessi ai medesimi, ha operato un rinvio pregiudiziale dinanzi alla Corte di giustizia: le due questioni riguardano tre aspetti di cruciale rilevanza, quali l'ambito territoriale di applicazione della direttiva 96/46 e della correlata normativa nazionale in materia di protezione dei dati, la qualificazione di Google come «responsabile del trattamento» ai sensi della medesima direttiva e, per quanto più concerne la presente analisi, la portata effettiva del diritto all'oblio come desumibile dagli indici normativi del diritto (allora) comunitario.

La causa, destinata a rappresentare un punto di riferimento irrinunciabile per le successive elaborazioni teoriche nonché per il concreto sviluppo delle tecnologie del settore — come dimostrato dalle misure di immediata applicabilità adottate a seguito della decisione — aveva suscitato profondo interesse sin dal momento della pubblicazione delle conclusioni dell'avvocato generale[57]: queste, infatti, come da

[55] Si veda, oltre a E. TOSI, *La responsabilità civile*, cit., in prospettiva più ampia R. PETRUSO, *Fatto illecito degli intermediari tecnici della rete e diritto d'autore: un'indagine di diritto comparato*, in *Europa e dir. priv.*, 2012, 4, p. 1175.
[56] Presentano i fatti all'interno di una panoramica più ampia O. POLLICINO – M. BASSINI, *Diritto all'oblio: i più recenti spunti ricostruttivi nella dimensione comparata ed europea*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, cit., pp. 208 ss.
[57] N. JÄÄSKINEN (Avvocato generale), *Opinion* in the case C-131/12, *Google Inc. c. Agencia Española de Protección de Datos*, 25 giugno 2013.

anticipazione, costituiscono spunto di riflessione per la pertinenza all'argomento qui trattato, in quanto, sebbene rese in merito a fatti cadenti sotto il sistema della direttiva e comunque prive di valore vincolante ai fini della sentenza, non possono non risentire dell'incombere dell'affermazione, se non normativa, concettuale e sociale, di particolari esigenze in materia di tutela della *privacy* in ambito informatico, una delle cui manifestazioni più emblematica è proprio il "diritto all'oblio".

Dopo aver tracciato un quadro sintetico ma cristallino dell'evoluzione storica del settore, l'avvocato perviene ad esprimere il proprio parere in merito al terzo quesito.

I rimedi predisposti dalla direttiva ammontano innanzitutto a quanto previsto dall'art. 12, lett. b): l'interessato ha diritto di ottenere dal responsabile del trattamento procedimenti quali «la rettifica, la cancellazione o il congelamento» delle informazioni, ma in via subordinata rispetto alle condizioni stabilite dalla disposizione stessa. Presupposto per l'esperimento di tali misure correttive e in senso lato cautelari è che il trattamento (per la cui definizione, qui cruciale, si fa riferimento all'art. 2, lett. b)) dei dati non sia «conforme alle disposizioni della presente direttiva». Il parametro indicato si riempie di significato mediante un collegamento con l'art. 6, appartenente alla Sezione rubricata «Principi relativi alla qualità dei dati» e, più in generale, con il Capo II della direttiva, il quale regola le «condizioni generali di liceità dei trattamenti di dati personali». In realtà, lo stesso art. 12 prevede un rinvio in qualche modo "rafforzato", laddove aggiunge, sempre alla lett. b), che la non conformità del trattamento debba risultare «in particolare a causa del carattere incompleto o inesatto dei dati», con ciò stabilendo un nesso testualmente esplicito con la lett. d) dell'art. 6, il quale simmetricamente dispone che «devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati […]».

Come si evince facilmente dai rapporti interni al testo normativo, la predisposizione di rimedi drastici nella facoltà dell'utente non risponde ad una logica arbitraria la cui determinazione è lasciata alla libera disponibilità del soggetto, ma si fonda su presupposti specifici, riconnessi alla violazione degli obblighi e dei divieti contenuti nella direttiva.

Una maggiore apertura potrebbe invece essere ravvisata nell'art. 14, lett. a) della direttiva: alla persona interessata è riconosciuto il diritto «di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano». Rispetto all'articolo citato in precedenza, se la protezione del soggetto gode di maggior respiro, altrettanto innegabilmente assai ampio è il margine di discrezionalità che residua per l'interprete, come dimostra la scelta esegetica dell'avvocato generale. Quest'ultimo ritiene che la sola preferenza soggettiva per la cancellazione di un

contenuto sgradito non costituisca un motivo legittimo o di tale preminenza da determinare la soccombenza degli interessi pubblici o di terzi di cui all'art. 7, lett. e) e f)[58].

In sintesi, nell'ambito concettuale di un eventuale "diritto all'oblio", la legislazione vigente offrirebbe una tutela in ordine ad un numero di ipotesi potenzialmente molto vasto, ma comunque riferibili alla violazione di specifiche previsioni relative ai requisiti di legittimità del trattamento, senza disporre alcun rimedio di ordine generale o che, pur soggetto a limitazioni soprattutto in considerazione del necessario bilanciamento con altri interessi fondamentali del singolo e della collettività, consenta all'individuo di rispondere con strumenti efficaci ai rischi sempre attuali che il carattere dinamico della rete Internet determina.

Secondo la prospettiva che l'avvocato generale imprime alla disciplina vigente, non è dunque ravvisabile un diritto per l'individuo di ottenere la cessazione della diffusione di dati personali che egli ritenga, in base a considerazioni puramente soggettive e che non trovano conforto in alcuna specifica disposizione di legge[59], astrattamente lesiva o contraria ai suoi interessi e dunque potenzialmente pregiudizievole. È dunque esito necessario del ragionamento concludere per la confutazione dell'esistenza di un "diritto all'oblio" nell'ambito dei diritti riconosciuti alla persona interessata dalla disciplina vigente in materia di tutela di dati personali[60].

Peraltro, è particolarmente significativo rilevare, da un punto di vista dell'effettività della tutela richiesta, che, stando all'esplicita notazione dell'avvocato generale, la riflessione teorica sull'ammissibilità di un diritto all'oblio perderebbe ogni rilevanza pratica nel caso di specie[61]: se, infatti, in modo concorde alle conclusioni, si ritiene che *Google* non vada considerato come «responsabile del trattamento», un'autorità nazionale per la protezione dei dati non potrebbe comunque imporre ad un fornitore di servizi di motore di ricerca su Internet di eliminare informazioni dal suo indice di risultati, fatte salve alcune specifiche ipotesi[62].

---

58 *AG's Opinion* C-131/12, parr. 106-108.

59 Le singole previsioni possono dettare divieti o obblighi specifici, così come utilizzare clausole generali: è il caso dell'art. 6, lett. a), il quale richiede che i dati siano trattati «lealmente». La trasposizione di tale regola nella normativa italiana di attuazione è avvenuta mediante adozione della dizione «secondo correttezza», versione più familiare al diritto nazionale e più vicina alla formula della "buona fede (oggettiva)". Indaga il rapporto tra liceità e correttezza e la loro interazione nel definire le regole di condotta *iure* nel trattamento dei dati personali E. NAVARRETTA, *Commento all'art. 11*, in C. M. BIANCA – F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196*, Cedam, 2007, pp. 251 ss.

60 *AG's Opinion* C-131/12, parr. 111 e 137.

61 *Ibidem*, par. 101.

62 *Ibidem*, parr. 99-100.

III.1. LA SUPPLENZA GIURISPRUDENZIALE DELLA CORTE DI GIUSTIZIA NELLA PROSPETTIVA DELLA TUTELA DEI DIRITTI FONDAMENTALI E L'INCOGNITA DELLE RICADUTE APPLICATIVE

Sebbene sia oltremodo complesso afferrarne la portata, data la pubblicazione solo recente e alla luce dei risultati fortemente originali cui essa perviene, è inevitabile dar conto della decisione della Corte di giustizia, astenendosi dal rendere un esaustivo commento per concentrarsi piuttosto sui principi di diritto e sui passaggi logici che più rilevano in questa sede[63].

Il ragionamento sotteso alla sentenza è percorso da due linee di tendenza convergenti il cui incontro segna la misura della notevole distanza dalle conclusioni dell'avvocato generale, le quali risultano, nella sostanza, in gran parte smentite: l'impostazione dei giudici si ispira, da un lato, alla stella polare del rispetto dei diritti fondamentali della persona sanciti (tra le altre) dalla Carta di Nizza, dall'altro, si fonda su una più che condivisibile valorizzazione della "realtà effettuale" del mondo di Internet vista attraverso il prisma giuridico.

Così, innanzitutto, non deve essere sottovalutato il momento della sussunzione del soggetto coinvolto nella categoria più idonea a descriverne l'operato e a consentire l'applicazione delle regole più coerenti con il dato concreto delle attività e dei poteri di fatto esercitati: pregevole, dunque (oltre che imprescindibile, per l'obiettivo chiaro al giudicante), la scelta di marcare la distinzione tra l'editore della pagina *web*–terzo e il gestore del motore di ricerca, *in primis*, alla luce dei dati forniti dall'esperienza, o meglio, dalla presa coscienza delle dinamiche effettive della rete[64], inoltre (secondo passaggio), alla stregua del parametro costituito proprio dall'«ingerenza […] nel diritto fondamentale al rispetto della vita della persona interessata»[65].

La Corte chiarisce che, nelle questioni di cui si dibatte, il ruolo di *Google* e delle figure affini merita di essere isolato, non tanto e non immediatamente per ragioni di giustizia sostanziale, bensì perché conseguenza della corretta interpretazione dei lineamenti dei destinatari delle prescrizioni della normativa comunitaria a tutela della *privacy*, in relazione alla quale i giudici di Lussemburgo svolgono appunto una funzione nomofilattica, oltre che, come palese nel caso di specie, adeguatrice rispetto ai mutamenti della realtà sociale.

---

63 Corte di giustizia UE, 13 maggio 2014, C-131/12, *Google Spain*, reperibile presso *www.curia.europa.eu*.

64 La Corte ha sempre dimostrato una particolare sensibilità nel cogliere le peculiarità delle fattispecie legate alla messa in rete di un contenuto: considerazioni analoghe sulla ubiquitarietà delle informazioni diffuse a mezzo Internet, sebbene a fini diversi, erano state svolte nella sentenza 25 ottobre 2011, nei procedimenti riuniti C-509/09 e C-161/10, *eDate Advertising*, richiamata dalla stessa pronuncia in esame. In quest'ultima, invece, il *distinguishing* di Lussemburgo ha compiuto un passo ulteriore, sostenendo una specifica dilatazione dell'accessibilità dei dati quando elaborati dagli algoritmi di un motore di ricerca e dunque un'autonoma rilevanza del ruolo di tali *service provider*: da questo argomento «strutturale» dissentono fortemente A. PALMIERI–R. PARDOLESI, *Diritto all'oblio: il futuro dietro le spalle*, in *Foro it.*, 2014, IV, cc. 317 ss., i quali giungono a parlare persino di «rigurgito antistorico e irrazionale». La posizione dei due Autori si segnala per il netto impianto critico, segnato da un'inquietudine di fondo tanto per i presupposti asseritamene ambigui su cui pare fondata la decisione quanto per i risultati cui essa perviene, e quindi per le conseguenze che dal quadro incerto così delineato potrebbero discendere in futuro.

65 Corte di giustizia UE, *Google Spain*, par. 87.

Logicamente, poi, sul piano della garanzia di una tutela utile, è dimostrato *a fortiori* che ciò che rileva sia l'eliminazione della causa degli effetti pregiudizievoli (vale a dire, la rimozione degli strumenti di diffusione del contenuto) effettuata dal soggetto da cui tali effetti scaturiscono (il motore di ricerca): una volta compreso il nesso che lega gli uni all'altro, non v'è più ostacolo all'accoglimento della soluzione proposta. In conclusione, data l'indipendenza tra le due posizioni, è del tutto ragionevole che la richiesta di cancellazione possa essere indirizzata verso il solo gestore senza essere subordinata né alla previa o simultanea cancellazione delle informazioni dalle pagine *web* di terzi né alla liceità delle loro pubblicazione su tali pagine[66].

Confermata così la necessità di operare peculiari adattamenti per attuare il "diritto all'oblio" su Internet, si pone la il problema (corrispondente alla terza questione pregiudiziale) dei presupposti in presenza dei quali l'interessato è legittimato a richiedere la rimozione e in capo al gestore sorge il relativo obbligo di operarsi a tal fine. Problema tutt'altro che secondario, anzi, sullo stesso livello del precedente, almeno in un contesto normativo che, come noto, è caratterizzato dall'assenza di una previsione generale che riconosca un preciso diritto in tal senso, il quale a sua volta non sembra neppure poter essere facilmente dedotto dalla logica e dai principi del sistema normativo vigente: e per lo "stato dell'arte" è sufficiente richiamare le limpide conclusioni dell'avvocato generale.

Il nodo del contrasto interpretativo presuppone che le informazioni oggetto della richiesta siano veritiere nonché legittimamente pubblicate: sulla scorta di ciò si tratta di verificare se, in base ad una serie di parametri determinati, con il passare del tempo la medesima pubblicazione (continuativamente in atto, secondo le ormai note dinamiche digitali) manifesti profili di illiceità tali da consentire l'attivazione dei meccanismi di cui agli artt. 12 e 14 della direttiva.

Il ragionamento della Corte sul punto può essere schematizzato come segue: innanzitutto, essa adotta un'interpretazione tendenzialmente estensiva della lettera della legge (art. 6, par. 1, lett. da c) a e)), ove valorizza l'aspetto temporale come dimensione in cui valutare se i dati sono «inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento»[67] e, di conseguenza, in cui individuare e misurare ulteriori ipotesi di incompatibilità del trattamento rispetto alle disposizioni della direttiva; dall'altra parte, si ricerca un parametro in base al quale riempire di significato il giudizio circa l'adeguatezza, la pertinenza e la non eccessività delle informazioni.

Tra le possibili opzioni che si presentano all'interprete nel compiere quest'ultima operazione spiccano quelle avanzate dal giudice *a quo*, consistenti rispettivamente nella circostanza che i dati in questione possano arrecare pregiudizio all'interessato e nel fatto che questo esprima una mera preferenza soggettiva nel senso della rimozione. Espressamente la Corte, con una statuizione di notevole

[66] *Ibidem*, par. 88.
[67] *Ibidem*, parr. 92-93.

importanza concettuale, respinge la tesi incentrata sulla potenzialità dannosa della permanenza dell'informazione nei risultati delle ricerche collegate al nome dell'interessato[68], per dare rilevanza ad un ben più pregnante parametro, la cui adozione smentisce in modo implicito la correttezza del secondo criterio addotto in sede di rinvio.

La sentenza stabilisce che l'inadeguatezza dei dati rispetto alle finalità del trattamento e, dunque, in definitiva, la legittimazione ad ottenere la cancellazione devono essere valutate nella più ampia ottica del diritto alla *privacy*, nella sua configurazione "attualizzata" rispetto al momento in cui si domanda la tutela: occorre appunto valutare «se l'interessato abbia diritto a che l'informazione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome»[69], vale a dire se, in relazione alla situazione presente, sussistano quelle condizioni che, ove riscontrate in origine, avrebbero condotto a ritenere prevalente la posizione di colui che agisce per la rimozione tanto da rendere illecita la pubblicazione.

L'appiglio normativo e sistematico è costituito, secondo quanto accennato, dai diritti fondamentali sanciti agli artt. 7 («rispetto della vita privata e della vita familiare») e 8 («protezione dei dati di carattere personale») della Carta di Nizza: in sostanza, nella lettura giurisprudenziale del "diritto all'oblio", stante l'assetto perlopiù indefinito di quest'ultimo, vengono in rilievo le disposizioni concernenti le due sfumature del diritto alla riservatezza, cui evidentemente si ritiene il primo possa essere ricondotto, in quanto, di fatto — si potrebbe ipotizzare — derivante da una semplice traslazione temporale degli interessi sottesi al riconoscimento del secondo.

Una volta intersecato il piano dei diritti della persona è immediato derivarne la conclusione necessaria, la quale si presenta come risultato anche pratico della decisione: la cancellazione potrà essere ottenuta soltanto ove si risolva a favore del richiedente il bilanciamento tra interessi in gioco, a prescindere, quindi, tanto dalla specifica circostanza che l'informazione arrechi un pregiudizio quanto, in pari misura, dal mero desiderio del soggetto cui i dati si riferiscono. Ciò — puntualizza la Corte — nonostante sia acclarato che «i diritti fondamentali […] prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico ad accedere all'informazione suddetta in occasione di una ricerca»[70]: sono infatti plausibili eccezioni alla regola generale legate alla preminenza (da verificarsi ad opera del giudice nazionale) del diritto di informazione, in relazione a quelle condizioni che secondo un'elaborazione ormai consolidata giustificano l'attenuazione o il venir meno delle esigenze di tutela della riservatezza.

[68] *Ibidem*, par. 96.
[69] *Ibidem*, par. 96.
[70] *Ibidem*, par. 99.

D'altra parte, la reviviscenza di una serie di parametri solitamente impiegati nell'ambito dei giudizi di bilanciamento che vedono tra gli interessi contrapposti il diritto alla *privacy* "originario" sembra avvalorare con forza la prospettiva sopra menzionata di inquadramento del diritto all'oblio, così come traspare dall'*iter* logico seguito dalla Corte: la riconduzione della posizione sostanziale collegata a quest'ultimo a situazioni soggettive già consolidate nella riflessione giuridica rappresenta un dato interpretativo che non può non essere valorizzato al fine di rendere meno incerto l'ormai cruciale giudizio di bilanciamento, intorno alle cui molteplici sfumature è destinato ad accendersi, anche in considerazione delle evidenti conseguenze pratiche, un vivace dibattito[71].

A tale proposito, in conclusione, si deve ribadire come, secondo l'impostazione adottata dalla Corte, la richiesta di cancellazione possa essere legittimamente diretta verso il motore di ricerca, a sua volta obbligato a rimuovere dall'indicizzazione dei risultati relativi al nome di una persona i *link* verso pagine *web* di terzi contenenti informazioni sull'interessato: ne discende che, in definitiva, quantomeno in prima istanza, sarà compito del gestore del motore di ricerca assumere una decisione circa l'ammissibilità della domanda, il cui esito dipenderà dai criteri adottati in sede di bilanciamento che lo stesso gestore — pur senza alcuna qualifica pubblica — sarà chiamato a svolgere, con il rischio di formazione di prassi contraddittorie al cospetto di diritti fondamentali della persona.

IV. QUALE «RIGHT TO BE FORGOTTEN» DOMANI IN EUROPA? IL PRESUNTO CARATTERE INNOVATIVO DELL'ART. 17 DELLA PROPOSTA DI REGOLAMENTO RISPETTO ALLE CONDIZIONI DI CANCELLAZIONE DEI DATI

Com'è facilmente desumibile, anche sulla scorta di considerazioni empiriche, il quadro così delineato mal si concilia con la esigenze pratiche attinenti al mondo digitale che abbiamo tentato di segnalare in precedenza con riferimento alla concreta configurazione di servizi della società dell'informazione e alle difficoltà di operare una rimozione dei dati personali presenti in rete, specialmente a fronte della necessità del loro conferimento ai fini dell'erogazione delle prestazioni richieste[72].

Per quanto concerne i motori di ricerca, sarebbe opportuno uno studio apposito che si concentri in via esclusiva sulle caratteristiche specifiche di questo tipo di intermediari, così da poter almeno tentare di

[71] Come esempio principe conviene citare il seguente: in seguito alla decisione della Corte, il motore di ricerca direttamente interessato dalla pronuncia (*Google*) ha istituito in Europa un gruppo di studio composto da esperti e professionisti del settore incaricato di approfondire la questione del bilanciamento tra diritti attraverso il confronto con le esperienze giuridiche di diversi Stati Membri, realizzato in appositi incontri pubblici. I contenuti e i risultati degli eventi organizzati sono reperibili presso il portale *www.google.com/advisorycouncil*.

[72] Problematiche tutte evidenziate in F. PIZZETTI, *Il prisma del diritto all'oblio*, cit., p. 41.

risolvere gli elementi di problematicità evidenziati dallo stesso avvocato generale nelle conclusioni in merito alla seconda questione pregiudiziale: valgano perciò le segnalazioni di aspetti critici fin qui evidenziati.

Le perplessità forse maggiori e senza dubbio giustificate su cui conviene concentrarsi in questa sede sorgono, invece, riguardo a quegli apparati informatici che rientrano senza difficoltà nell'ambito del *cloud computing*, per i quali già sono stati evidenziati i tratti salienti degli ostacoli di fatto alla tutela dell'interesse del singolo alla rimozione dei propri dati personali; inoltre, per quanto riguarda i fornitori di questo tipo di servizi, non può essere esclusa la loro qualificazione in termini di *controller* e dunque la configurazione di speciali responsabilità attinenti al trattamento dei dati[73].

A fronte di una insicurezza diffusa tra gli utenti di Internet in materia di *privacy* e della percezione altrettanto vasta della necessità di rivelare informazioni personali come parte integrante della vita moderna o come condizione indispensabile per fruire dei servizi *online*[74], l'emergere dell'esigenza della cancellazione dei dati è stato inevitabile lo scontro con il panorama offerto dalla direttiva 95/46, di cui si è avuto modo di constatare l'insufficienza.

L'Unione europea (ambito a cui limitiamo la presente indagine, potenzialmente già assai vasta), nell'intraprendere una strada di riforma complessiva delle regole a tutela dei dati personali ha esplicitamente posto tra i suoi obiettivi[75] l'introduzione di un "diritto all'oblio", il quale è stato poi incorporato nell'art. 17 della Proposta di regolamento come «diritto all'oblio e alla cancellazione».

Senza pretesa di esaustività, può essere interessante tentare di incrociare gli aspetti tecnico-pratici evidenziati in precedenza con lo spettro applicativo della disposizione in esame per quello che può risultare dai caratteri essenziali dell'enunciato normativo, una cui effettiva concretizzazione dipenderà, è bene ricordarlo, dall'interpretazione che ne daranno le corti nazionali e, in particolar modo, la Corte di giustizia dal momento in cui il regolamento entrerà in vigore, ponendosi dunque come diritto unico a livello europeo: pertanto, in questa sede non ci si potrà spingere molto oltre la verifica di una generica adeguatezza degli strumenti riconosciuti dalla nuova disciplina e ci si limiterà a segnalare possibili casi di incongruenza tra la tutela apprestata e i problemi rilevanti del contesto specifico che qui interessa, ossia la protezione dei dati personali nella tecnologia del *cloud computing*.

Le fondamenta su cui si sviluppa l'art. 17 sono costituite, come detto, da una precisa scelta legislativa, realizzata nel riconoscimento all'interessato di un vero e proprio diritto, il quale include la facoltà per il

[73] Sul punto è incentrata gran parte del contributo di P. BALBONI – L. BOLOGNINI – D. FULCO – E. PELINO, *Cloud computing e tutela dei dati personali in Italia: una sfida d'esempio per l'Europa*, in *Diritto, economia e tecnologie della privacy*, Istituto Italiano per la Privacy, numero speciale settembre 2011.

[74] Si consulti il copioso materiale statistico riportate in Special Eurobarometer 359, *Attitudes on Data Protection and Electronic Identity*, giugno 2011: il periodo d'indagine è riferito a novembre-dicembre 2010.

[75] Oltre ai già citati opuscoli informativi della Commissione e alle dichiarazioni del Vice-presidente Reding, si vedano i considerando 53-54 della Proposta di regolamento.

soggetto «di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia ad un'ulteriore diffusione di tali dati» (par. 1). Il regolamento si pone dunque in un'ottica di doppia tutela, non ponendosi soltanto come inibizione alla ripetizione di comportamenti alla cui esecuzione l'interessato, evidentemente, ha ricollegato conseguenze a sé sfavorevoli, tanto da formulare la richiesta di cancellazione, ma andando a colpire e travolgere (sempre che ne ricorrano i requisiti) anche i trattamenti pregressi, o meglio, i risultati di questi ovvero il materiale stesso di possibili trattamenti futuri.

Una soluzione simile è resa quasi necessaria dalla necessità di confrontarsi con le caratteristiche della realtà informatica: da un lato, infatti, la rimozione dei dati conferiti impedisce alla radice il verificarsi di ulteriori operazioni che li abbiano ad oggetto ai fini più vari e conducano ad esiti pregiudizievoli per il soggetto, dall'altro il ragionamento che conduce all'opzione della cancellazione è, di necessità, consequenziale alla riflessione in base alla quale la mera presenza di un'informazione in rete può accedere ad una soglia di pericolosità percepita sufficiente perché ne sia richiesta l'eliminazione in quanto strumento di tutela da forme di lesione di situazioni giuridiche di particolare valore, spesso appartenenti al novero dei diritti fondamentali della persona, come nel caso della *privacy*.

Le riflessioni precedenti sono tanto più opportune per quanto riguarda i servizi *cloud*, dal momento che tra i rischi collegati al loro impiego si è menzionato il fatto che le informazioni siano conservate in *server* di rilevanti dimensioni insieme a quelle di miriadi di altri utenti e che siano rese accessibili anche a terzi, prestatori di servizi ausiliari ed incaricati di trattamenti ulteriori, con i quali è pure possibile che l'utente non venga mai a contatto: in tali ipotesi, finché il dato rimane memorizzato nel sistema del *provider* originario, è sempre possibile che esso sia conoscibile da parte di soggetti esterni, e l'obiettivo di tutela della situazione giuridica di volta in volta rilevante, minacciata proprio dalla reperibilità dell'informazione, ne risulta minata alla radice.

L'operatività del rimedio della cancellazione è prevista in coincidenza del ricorrere di quattro situazioni, le quali completano la definizione della struttura dell'art. 17 e tre delle quali risultano particolarmente significative in questa sede. Innanzitutto, la disposizione in esame provvede ad incorporare una categoria di ipotesi già presente nella direttiva in vigore, inserendola in un quadro sistematico insieme ad altri presupposti ai quali è ricollegata una doppia forma di tutela: la cancellazione e la rinuncia ad un'ulteriore diffusione dei dati possono infatti essere invocate quando «il trattamento dei dati non è conforme al presente regolamento […]» (par 1, lett. d)).

Questa condizione di applicazione, come dimostra l'inciso finale («[non conforme] per altri motivi») e la collocazione a chiusura del paragrafo, assume, in contrasto con il panorama precedente, una valenza onnicomprensiva ma, per questo, residuale: senza dubbio, essa costituisce il mezzo per salvaguardare

l'interessato in tutti i casi di generica infrazione della disciplina dettata a protezione dei suoi dati personali e dunque pare godere di un raggio d'azione potenzialmente vastissimo; d'altra parte, però, è plausibile che la volontà legislativa abbia concepito questo presupposto come cerniera del sistema, atta ad assicurare uno *standard* minimo di tutela, procurandosi invece di portare in primo piano, segnalandole specificamente e in modo distinto, quasi a rimarcarne l'importanza (oltre che a riconoscerne implicitamente o, forse, ad auspicarne la maggiore frequenza), altre ipotesi e motivi idonei a fondare la pretesa della cancellazione.

La disciplina vigente, al contrario, attribuisce rilievo centrale alla "non conformità" quale principale criterio di legittimazione della facoltà dell'interessato di chiedere l'eliminazione dei dati[76], e ne rafforza il valore nelle occasioni in cui essa si verifichi «a causa del carattere incompleto o inesatto dei dati»[77]. Se, come visto, l'art. 12 della direttiva rappresenta il fulcro normativo cui fare riferimento, nel regime attuale, per rintracciare un modello pur vago di "diritto all'oblio" (indagine che tende a concludersi con esiti negativi) e se ulteriori appigli in tal senso non possono essere individuati altrove con sufficiente chiarezza[78], un attento osservatore non dovrebbe sottovalutare il pregio della disciplina nazionale di recepimento, la quale, con una scelta parzialmente diversa dal legislatore comunitario, compie una diversa specificazione del presupposto di "non conformità", con il risultato (si può presumere consapevole) di far emergere una ben distinta ipotesi idonea a fondare la pretesa alla cancellazione, laddove la direttiva appare invece non del tutto perspicua.

È il caso dell'art. 7 del d. lgs. 196/2003, il quale, al comma 3, recita infatti: «L'interessato ha diritto di ottenere: […] b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati». Non v'è dubbio, leggendo i due testi normativi, che l'adeguamento del diritto interno sia stato condotto in piena ottemperanza alle indicazioni di risultato contenute nella direttiva. Per quanto riguarda, infatti, l'incompletezza o l'inesattezza dei dati, l'art. 7 presenta, al comma 3, una apposita lett. a), la quale prevede uno specifico rimedio di notevole coerenza, in considerazione della natura di quell'aspetto del dato (la corrispondenza a verità) alla cui tutela è preposto il parametro legislativo violato: all'interessato è pertanto riconosciuto il diritto di ottenere «l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati». D'altra parte — ed è questo il passaggio più interessante, per gli sviluppi futuri — tra le disposizioni della direttiva alla cui violazione è riconnesso l'obbligo per gli Stati membri di garantire al soggetto il diritto di ottenere la cancellazione, ben può e deve figurare il suddetto art. 6, con riferimento

[76] Questo diritto rientra tra i mezzi di tutela «forte», intesi appunto come reazione «alla violazione di una delle regole di liceità del trattamento […] oppure della clausola della correttezza»: E. BARGELLI, *Commento all'art. 7*, in C. M. BIANCA – F. D. BUSNELLI (a cura di), *Commentario al D. Lgs. 30 giugno 2003, n. 196*, p. 131.
[77] Così il già citato art. 12, par. 1, lett. b), in fine, della direttiva 95/46.
[78] Si vedano le conclusioni dell'avvocato generale nella causa C-131/12, discusse *supra*.

non solo alla lett. d), ma anche, in posizione non secondaria, come apprezzabilmente evidenziato dalla disciplina nazionale, alle lett. b), c) ed e).

Dalla lettura coordinata di queste disposizioni si coglie un nesso diretto, quasi essenziale, tra la liceità del trattamento dei dati e la finalità di quest'ultimo[79]: lo scopo viene appunto in rilievo, per espressa previsione normativa, da un lato quale forma di legittimazione — sia in modo puntuale, al momento della rilevazione, sia come criterio direttivo del trattamento nel suo complesso[80] — dall'altro quale parametro di adeguatezza della qualità dei dati[81], da verificarsi lungo tutta la durata del trattamento, nonché come limite operante sul piano temporale[82].

Avvalendosi dell'interpretazione implicita che ne dà l'atto delegato di recepimento tramite il riferimento testuale agli «scopi per i quali i dati sono stati raccolti o successivamente trattati», si può così affermare che il combinato disposto degli artt. 6 e 12 della dir. 95/46 imprime alla disciplina comunitaria una connotazione tale per cui «all'interno del parametro della liceità del trattamento dei dati spicca quale fondamentale criterio ispirativo il principio di finalità»[83]. Questa impostazione pare confermata in pieno dalla proposta di regolamento, laddove il caso in cui «i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati» corrisponde ad una delle condizioni puntualmente elencate che fondano il diritto alla cancellazione dei dati (art. 17, par. 1, lett. a)), con il risultato che, in ipotesi di violazione del principio citato, l'interessato può usufruire di una forma particolarmente radicale di tutela inibitoria, sia inibitoria sia preventiva.

Il c.d. *purpose limitation principle*[84], dunque, oltre a costituire criterio di selezione e di utilizzo dei dati[85], contribuisce a definire in senso sostanziale i contorni della posizione di diritto contrapposta alla tutela dell'interessato[86] e si presta quale elemento centrale intorno al quale costruire un efficiente sistema di protezione dei dati personali, specialmente laddove ne sia assicurato il raccordo con l'istituto del consenso informato, che ne rappresenta una sorta di "negativo".

---

79 Nesso che si riverbera ed emerge specularmente nell'ambito del consenso: possono essere trattati i dati solo per certe finalità, perché per quelle si è prestato il consenso: v. *infra*.

80 I dati personali, a norma dell'art. 6, par. 1, della direttiva, devono essere «rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità» (lett. b)).

81 «[I dati devono essere] adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati» (art. 6, par. 1, lett. c)).

82 «[I dati devono essere] conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati» (art. 6, par. 1, lett. e)).

83 Cfr. E. NAVARRETTA, *Commento all'art. 11*, cit., p. 264.

84 Approfondimenti in ART. 29 WP, *Opinion 3/2013 on purpose limitation*, WP203, adottata il 2 aprile 2013. Il principio consente di raggiungere un equilibrio tra esigenze di affidamento e certezza giuridica da un lato e di flessibilità nel trattamento dei dati dall'altro, e a tal fine è costruito su due blocchi concettuali ben distinti: si tratta appunto delle nozioni «*purpose specification*» («i dati personali devono essere […] rilevati per finalità determinate, esplicite e legittime») e di «*compatible use*» («i dati personali devono essere […] successivamente trattati in modo non incompatibile con tali finalità»).

85 Nell'ambito della valutazione della sussistenza delle condizioni che legittimano una richiesta di cancellazione da parte dell'interessato, la definizione delle finalità del trattamento ai sensi dell'art. 6, par. 1, lett. b) diventa pregiudiziale per attivare il giudizio di proporzionalità di cui alla lett. c) e rendere operante il criterio temporale di cui alla lett. e): cfr. ART. 29 WP, *Opinion 3/2013*, cit., par. II.2.1.

86 E. NAVARRETTA, *Commento all'art. 11*, cit., p. 267.

Infine, ai sensi dell'art. 17, par. 1, lett. b) del regolamento, la cancellazione dei dati e la rinuncia a ulteriori diffusioni possono essere ottenute dall'interessato quando il medesimo «revoca il consenso su cui si fonda il trattamento»: il legislatore europeo, per queste ipotesi, supplisce al silenzio[87] che caratterizza la direttiva sotto il profilo delle conseguenze rispetto alla scelta del soggetto il quale non ritenga più opportuna la prosecuzione del trattamento al quale aveva in origine acconsentito, e al contempo attribuisce all'interessato una posizione primaria di controllo.

La previsione di un diritto alla cancellazione conseguente alla revoca del consenso è infatti operata in piena coerenza con il ruolo che il regolamento attribuisce al consenso. Il rinvio della lettera in esame all'art. 6, par. 1, lett. a) della proposta di regolamento, infatti, non deve leggersi secondo la prospettiva riduttiva di mero riferimento interno dal valore solo testuale o formale, poiché non si può ignorare il disegno complessivo dell'art. 6, il quale dispone che «[i]l trattamento dei dati personali è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni […]», tra cui rientra, appunto, il caso in cui «l'interessato ha manifestato il consenso al trattamento dei propri dati personali per una o più specifiche finalità»[88] (lett. a)). In aggiunta, esplorando ancora più a fondo il panorama del regolamento, conviene completare il quadro concettuale con la citazione del primo comma dell'art. 7, par. 3, in base al quale l'interessato «ha il diritto di revocare il proprio consenso in qualsiasi momento»: alla luce di ciò, l'interprete può trarre due conclusioni.

Per quanto riguarda la prima, si può affermare che il consenso del soggetto a cui i dati si riferiscono diventa il perno attorno al quale è costruito l'intero sistema del conferimento volontario di dati, la cui gestione concreta, anche in fasi successive all'inizio del trattamento, è rimessa alla libera determinazione dell'interessato[89], anche mediante la facoltà di revoca[90] cui adesso si collega, ai sensi dell'art. 17, la cancellazione dei dati. In questa ottica, dunque, si conclude che il consenso, quale elemento strutturale, deve (si tratta chiaramente di necessità logico-giuridica) rimanere fermo ed accompagnare il trattamento per tutta la sua durata.

La seconda riflessione è strettamente collegata alla precedente. Nell'art. 17, par. 1, lett. b) l'ipotesi della revoca del consenso, per quanto evidenziata attraverso una previsione distinta, potrebbe essere considerata nient'altro che specificazione del requisito *sub* d) — il quale di per sé sarebbe sufficiente (come visto) a coprire un vasto numero di casi — dal momento che, alla pari della disciplina attuale, il consenso figura comunque tra le condizioni necessarie per il trattamento e, pertanto, la sua mancanza integra senza dubbio una "non conformità" rispetto al testo normativo, idonea a giustificare il rimedio previsto per evenienze di questo genere, indipendentemente dalla specifica esemplificazione delle

[87] Così si esprimono M. L. AMBROSE – J. AUSLOOS, *The Right to Be Forgotten Across the Pond*, in *Journal of Information Policy*, 2013, 3, 7.
[88] Si noti il riferimento al principio di finalità, dimostrazione della stretta correlazione con il consenso, cui si accennava in precedenza.
[89] Il tema è stato oggetto di studio in Art. 29 WP, *Opinion 15/2011 on the definition of consent*, WP187, adottata il 13 luglio 2011, par. II.3, dove si afferma chiaramente: «*Consent is related to the concept of informational self-determination*».
[90] Cfr. *ibidem*: «*The notion of control is also linked to the fact that the data subject should be able to withdraw his consent*».

medesime[91]. La vera novità, dunque, consisterebbe piuttosto nel riconoscimento di un pieno diritto di ritirare il consenso originariamente prestato, da esercitarsi senza limiti temporali[92]: attraverso questo strumento flessibile ed ampio raggio d'azione si assicura all'interessato la possibilità di svolgere autonome valutazioni dei rischi legati al trattamento e di essere sempre in condizione di fare eventualmente seguire a queste, in base ad una decisione strettamente personale, l'interruzione del trattamento con la forma correlata di tutela individuata proprio nella nascita in capo al medesimo soggetto di un diritto alla cancellazione.

SEZIONE III

IPOTESI APPLICATIVE DELL'ART. 17 DELLA GDPR AI SERVIZI DI CLOUD COMPUTING: UN'ANALISI PROSPETTICA

V. PRINCIPALI CRITICITÀ RICORRENTI NEL PASSAGGIO ALLA LAW IN ACTION

V.1. LA QUESTIONE PREGIUDIZIALE DELLA QUALIFICAZIONE GIURIDICA DEI SOGGETTI COINVOLTI

Le considerazioni appena svolte potrebbero diventare fonti di ulteriori problemi una volta trasferite sul piano concreto dei servizi di *cloud computing*. Innanzitutto, per quanto riguarda il *purpose limitation principle*, appare arduo stabilire le finalità per le quali i dati sono stati raccolti o trattati e rispetto alle quali deve essere valutata la pertinenza delle informazioni conferite: ciò, principalmente, non per la mancata indicazione di tali finalità al momento dell'accettazione delle "condizioni di servizio"[93], bensì per il loro

[91] In realtà, il passaggio non è scontato, dal momento che sotto il regime attuale, in cui pure vale la regola della cancellazione dei dati in caso di trattamento non conforme alle disposizioni della direttiva, un'autorevole posizione (ART. 29 WP, *Opinion 15/2011*, loc. cit.) afferma: «*withdrawal is not retroactive, but it should, as a principle, prevent any further processing of the individual's data by the controller*»; non si spinge più in là il d. lgs. 196/2003 laddove stabilisce, all'art. 11, comma 2: «I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati». Con una scelta consapevolmente in contrasto con la giurisprudenza del Garante, sostiene la possibilità per l'interessato di chiedere non solo la cessazione *ex nunc* del trattamento, ma anche la cancellazione a seguito della revoca del consenso/opposizione E. BARGELLI, *Commento all'art. 7*, cit., p. 137.

[92] Peraltro, lo stesso art. 7, par. 3 della proposta di regolamento aggiunge, al secondo periodo, per quanto riguarda gli effetti della revoca, che essa «non pregiudica la liceità del trattamento basata sul consenso prima della revoca». Si noti che la norma potrebbe essere interpretata *a contrario* nel senso che i trattamenti successivi alla revoca sono necessariamente illeciti (sempre che, com'è ovvio, non siano fondati su una delle altre condizioni di cui all'art. 6): in questa ottica risulta avvalorata la tesi a favore della possibilità di ricomprendere i casi di revoca del consenso cui ricollegare il diritto alla cancellazione nella categoria delle ipotesi di "non conformità" alle disposizioni del regolamento.

[93] Evenienza in cui il trattamento avverrebbe in violazione delle disposizioni sull'informazione dell'interessato (v. art. 14 della proposta di regolamento e art. 10 dir. 95/46): si ricadrebbe, ancora una volta, nelle ipotesi *sub* d).

carattere intrinsecamente indefinito e vago[94], soprattutto se attinenti all'implementazione delle attività relazionali dell'individuo, ovvero fondamentalmente indeterminabile, come, più in generale, nei casi in cui il servizio abbia ad oggetto la condivisione di informazioni e contenuti prodotti dall'utente o forniti dall'interessato[95].

Probabilmente, così, sarebbe assai arduo richiedere la cancellazione dei dati conferiti se il regolamento non includesse una previsione autonoma, almeno sul piano formale, per i casi di revoca del consenso: in questo modo, invece, l'interessato può, senza il rischio di incorrere in controversie relative all'interpretazione della "non conformità" del trattamento, ottenere la rimozione delle informazioni che lo riguardano mediante una semplice manifestazione unilaterale di volontà.

In realtà, la questione dell'applicazione dell'art. 17 al *cloud computing*, in assenza di interventi della giurisprudenza a causa della novità del fenomeno e, più semplicemente, della natura ancora non vincolante del regolamento, costituisce un nodo inestricabile se affrontato in via puramente astratta e non coordinata con le esigenze pratiche degli utenti e le circostanze concrete dei diversi servizi.

Così, ai fini di un più perspicuo inquadramento delle prospettive di cancellazione di dati ormai parte dell'infrastruttura digitale, potrebbe forse risultare vantaggioso prendere le mosse anche dall'esame del comportamento materiale dell'interessato e di altri soggetti che entrano in collegamento, diretto o indiretto, con il medesimo: in particolare, in questa sede, viene alla mente la possibilità di condurre una breve analisi degli spazi di azione e delle dinamiche operative dell'introducendo "diritto all'oblio" in ipotesi specifiche, distinte sulla base delle modalità di immissione dell'informazione nel flusso digitale e sull'origine dei dati[96].

Lo schema al quale si fa riferimento si compone di tre interrogativi, ciascuno corrispondente ad una precisa situazione problematica di coinvolgimento di informazioni di vario genere in rete: «1) *If I post something online, should I have the right to delete it again?*; 2) *If I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it?*; 3) *If someone else posts something about me, should I have the right to delete it?*».

Nonostante la prospettiva indubbiamente suggestiva, una serie di ragioni impedisce una diretta e piena trasposizione dei quesiti nella realtà del *cloud computing*, prime tra tutte le considerazioni per cui, nei

94 Particolarmente efficace l'osservazione in ART. 29 WP, *Opinion 3/2013*, cit., par. III.1.1., in merito di «*specified purposes*»: «*a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purpose', 'IT-security purposes' or 'future research' will – without more detail – usually not meet the criteria of being 'specific'*».

95 Cfr. ART. 29 WP, *Parere 5/2012*, cit., par. 3.4.1.2: «Poiché un tipico scenario di servizi *cloud* può facilmente coinvolgere un maggior numero di subcontraenti, il rischio del trattamento dei dati personali per ulteriori finalità incompatibili dev'essere considerato particolarmente alto». Non si esclude comunque che in tal caso ci si riconduca ad un'ipotesi di trattamento illecito.

96 Il riferimento è allo spunto offerto dai tre interrogativi (eminentemente pratici ma per ciò di indubbia rilevanza) avanzati, in materia di diritto all'oblio, da P. FLEISCHER (Google's Global Privacy Counsel), *Foggy thinking about the Right to Oblivion*, reperibile presso il suo blog *Peter Fleischer: Privacy…?*, 9 marzo 2011.

servizi di questo genere, da un lato il panorama dei soggetti in gioco è molto più complesso, dall'altro è necessario identificare correttamente cosa costituisca "*post*".

Come si evince chiaramente a seguito di una attenta riflessione, la chiave per affrontare in modo sistematico gli interrogativi proposti risulta nuovamente quella già indicata in più occasioni: invero, l'analisi risulterebbe notevolmente agevolata un volta definite a livello concettuale le nozioni di *data subject, controller e processor*, poiché il successivo passaggio ermeneutico, costituito dall'applicazione di questa suddivisione ai soggetti della fattispecie rilevante, renderebbe più rapida la distribuzione dei diritti e degli obblighi previsti dalla disciplina in materia di tutela dei dati personali e una riflessione sull'equilibrio così raggiunto tra gli interessi in gioco.

A tale riguardo, nell'ambito del *cloud computing* si può notare una incongruenza che rende all'interprete particolarmente ostica o quantomeno problematica e incerta l'applicazione dell'art. 17 della proposta di regolamento.

Quest'ultimo presuppone implicitamente una distinzione netta (quasi una contrapposizione) tra interessato o *data subject* («la persona fisica identificata o identificabile […]»: art. 4, n. 1), e responsabile del trattamento o *controller* (colui che «determina le finalità, le condizioni e i mezzi del trattamento dei dati personali»: art. 4, n. 5), ponendo in capo al secondo, come noto, l'obbligo di cancellare i dati personali del primo e di rinunciare ad una loro ulteriore diffusione.

Per quanto concerne i servizi *cloud*, è autorevole opinione del Gruppo di lavoro Art. 29[97] che «il cliente *cloud* determina la finalità ultima del trattamento e decide in merito all'esternalizzazione di tale trattamento e alla delega ad un'organizzazione esterna delle attività di trattamento»: «il cliente *cloud* agisce pertanto in qualità di responsabile del trattamento dei dati», tanto che da ciò gliene deriva la responsabilità per l'osservanza della disciplina rilevante in materia. A sua volta, il prestatore di servizi *cloud*, «quando fornisce gli strumenti e la piattaforma, agendo per conto del cliente […], è considerato alla stregua di un incaricato del trattamento».

Coordinando i due aspetti della questione, ne emerge un quadro piuttosto oscuro ed ellittico allo stesso tempo. Il soggetto che determini le finalità e i mezzi del trattamento dei dati di un soggetto terzo e che per fare ciò utilizzi un sistema *cloud* risulta tenuto a procedere alla cancellazione di tali dati, quando ricorrano le condizioni di cui alle lettere da a) a d) del par. 1: in questa ottica la disciplina dettata dal regolamento pare ignorare le problematiche relative all'impiego della tecnologia in esame, poiché assume come scontato quanto finora si è detto invece rappresentare un punto critico particolarmente delicato.

[97] V. ART. 29 WP, *Parere 5/2012*, cit., par. 3.3.1.

Si consideri infatti la seguente situazione: è pur vero che al momento della scelta del servizio il cliente-responsabile «deve scegliere un fornitore *cloud* che garantisca l'osservanza della normativa in materia di dati personali»[98], soprattutto con riguardo alle misure tecniche e organizzative di sicurezza, all'accesso e alla divulgazione non autorizzati[99] e ai trasferimenti internazionali delle informazioni, ma ciò non impedisce comunque che lo stesso cliente-responsabile, a causa della natura della tecnologia in questione, possa perdere il controllo sui dati conferiti da varie fonti, rischio appunto sempre possibile quando il trattamento sia effettuato tramite un servizio erogato in modalità *cloud*. Il cliente, dato il suo ruolo di *controller*, sarà indubbiamente responsabile nei confronti dell'interessato per eventuali violazioni del suo diritto alla riservatezza o per la mancata rimozione dei dati, ma l'impianto dell'art. 17, par. 1, per quanto generoso in termini di legittimazione alla pretesa di cancellazione, non risulta idoneo ad apprestare tutela effettiva al *data subject* nei casi in cui le informazioni non siano più sotto il raggio d'azione (esclusivo) del cliente del servizio *cloud*.

Parimenti, non risulta chiara la situazione in cui i dati conferiti siano riferibili proprio al cliente del servizio *cloud*, il quale diventa a sua volta "interessato": posto che in tale occasione non si registrerebbe comunque nessuno scollamento tra la fase di ponderazione degli interessi sottostanti alla richiesta di cancellazione da parte del soggetto e l'esecuzione di quest'ultima ad opera del medesimo (e sarebbe dunque superfluo riconoscere un diritto di pretesa verso se stessi), la portata della tutela garantita dal regolamento dovrebbe a maggior ragione essere valutata sul piano delle possibilità concrete di rimozione delle informazioni, tutela che però, come dimostrato, appare assolutamente depotenziata per motivi di ordine pratico–applicativo.

Invero, a parere di chi scrive, considerata la multiformità e la flessibilità delle prestazioni *online*, alla luce della concreta configurazione delle attività del fornitore del servizio, spesso connotate da una evidente "propositività" e fondate sull'innegabile impiego delle informazioni per finalità di profitto, sebbene in qualche modo vantaggiose anche per gli utenti, le ipotesi in cui il *provider* può essere qualificato come "responsabile del trattamento" rappresentano un numero significativo, e senza dubbio coinvolgono i protagonisti del mondo della rete[100]. A riprova della tesi qui avanzata, inoltre, potrebbe poi addursi che nei casi ora descritti il *provider-controller* si troverebbe, per non trascurabili ragioni di ordine sia tecnico sia economico, nella posizione migliore per procedere all'esecuzione dei rimedi di cui all'art. 17.

---

98 *Ibidem*.

99 Emerge in proposito il già citato art. 30, par. 2, della proposta di regolamento, il quale peraltro, come pure sottolineato, si rivolge sia al responsabile del trattamento sia all'incaricato del trattamento.

100 Da segnalare che lo stesso ART. 29 WP, *Parere 5/2009 sui* social network on-line, WP163, adottato il 12 giugno 2009, par. 3.1, riconosce che «i fornitori di SNS sono i responsabili del trattamento ai sensi della direttiva sulla protezione dei dati», in quanto «mettono a disposizione i mezzi per l'elaborazione dei dati degli utenti […], forniscono tutti i servizi di base relativi alla gestione degli utenti [e determinano] il modo in cui i dati degli utenti possono essere usati a fini pubblicitari e commerciali — inclusa la pubblicità fornita da terzi». Lo studio di queste piattaforme, estremamente diffuse nella società dell'informazione, risulta un valido banco di prova per l'applicazione della disciplina in materia di tutela dei dati personali al fenomeno in esame, poiché non si vedono ragioni valide per negare che esse ricalchino caratteristiche tipiche (o, quantomeno, lo schema funzionale essenziale) dei servizi di *cloud computing*.

Tuttavia, come visto, deve registrarsi la specifica presa di posizione del Gruppo di lavoro Art. 29, il quale non sembra particolarmente favorevole ad una simile prospettiva, propendendo per la qualificazione del cliente, anziché del fornitore, come responsabile del trattamento. Proprio sulla base di questa impostazione si è svolto il ragionamento precedente constatando le lacune (o meglio, la non piena efficacia) del par. 1 della disposizione in esame rispetto alle esigenze concrete del fenomeno del *cloud computing*: se davvero i soggetti in gioco rispondono ai ruoli di cui si è detto, sembrerebbe quasi che il legislatore europeo, per quanto innovativo sul piano dei diritti (astrattamente) riconosciuti al singolo, abbia ignorato il piano della loro applicazione in uno scenario fortemente segnato da nuovi e incalzanti sviluppi tecnologici.

V.2. IL SIGNIFICATO DEL PAR. 2 COME TIMIDA APERTURA A FORME DI REGOLAZIONE IN LINEA CON LE DINAMICHE DELLA REALTÀ INFORMATICA

La presunta "insensibilità" del regolamento alle complesse questioni poste dal mondo di Internet è attenuata dal par. 2 dello stesso art. 17, attraverso il quale può essere meglio valutata l'efficacia della proposta di regolamento ai fini dell'elaborazione di una risposta soddisfacente in tema di "diritto all'oblio", anche con riguardo al *cloud computing*[101].

Il testo prevede infatti: «Quando ha reso pubblici i dati personali, il responsabile del trattamento di cui al paragrafo 1 prende 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. Se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto responsabile di tale pubblicazione».

È innanzitutto necessario precisare come la disposizione prefiguri, visti i suoi riferimenti lessicali e, in generale, la sua ricchezza testuale, uno spettro applicativo non meno vasto rispetto alle molteplici interpretazioni che ne potranno essere rese dalla giurisprudenza, la quale è auspicabile che intervenga, una volta entrato in vigore il regolamento, a chiarire in modo dettagliato il contenuto di un enunciato di valore particolarmente significativo, anche ad una prima lettura. Per questi motivi le notazioni che seguono, lungi dalla pretesa di sostituirsi ad una più competente ermeneutica, avranno come scopo solo

[101] «*The innovative aspect of the proposed rules does not regard the right granted to the individual, but the different rules concerning the extension of the protection offered in relation to the new electronic ways of disseminating information*»: così, tra i pochi commentatori attenti alla nuova disposizione, A. MANTELERO, *U.S. Concern about the European Right to Be Forgotten and Free Speech: Much Ado About Nothing?*, in *Contr. e impresa/Europa*, 2012, 2, p. 735.

quello di fornirne una prima ipotesi di applicazione e di segnalare profili di speciale interesse in relazione al tema trattato.

Confrontando il par. 1 con il par. 2, la fattispecie considerata in quest'ultimo risulta marcatamente diversa, poiché il trattamento dei dati ad opera del responsabile ha assunto una particolare configurazione, in base alla quale si è determinata la pubblicità delle informazioni conferite, vale a dire (si può ipotizzare) ne è stata resa possibile l'accessibilità ad un più o meno ampio novero di soggetti indeterminati. L'ipotesi non è peregrina nell'ambito del *cloud computing*, poiché può accadere che ciò sia addirittura l'esito di una specifica scelta dell'interessato (come pure dell'utente con il consenso di quest'ultimo) a monte del singolo trattamento ovvero il risultato naturale di un determinato tipo di servizio che ha ricevuto in origine l'approvazione dell'interessato stesso[102].

Il regolamento completa dunque il par. 1, determinando quali siano le conseguenze di una richiesta di cancellazione che intervenga nell'ipotesi assai diffusa della condivisione con il pubblico dei dati conferiti. La previsione risulta assai calzante nella società dell'informazione e, soprattutto, nel mondo di Internet, dove la digitalizzazione e la connessione in rete semplifica la memorizzazione e favorisce una rapida circolazione dei dati, facendo aumentare il rischio di trattamenti ulteriori ad opera di terzi per finalità e con modalità spesso non soggette ad alcun controllo: se all'interessato è riconosciuto il diritto di ottenere la cancellazione dei dati e ne ricorrono i presupposti definiti per legge, è plausibile che egli possa ritenere le medesime ragioni che sottostanno alla richiesta rivolta al responsabile (legate, ad esempio, alla convinzione che un'informazione risulti a sé pregiudizievole) valide anche con riferimento alla detenzione dei medesimi dati da parte di soggetti terzi.

In tal caso, la previsione di un obbligo ulteriore in capo al *controller* è giustificato dal nesso funzionale (e causale) costituito dalla responsabilità nella pubblicazione dei dati: egli è tenuto a compiere una serie di attività la cui valutazione è affidata al parametro (di stampo prettamente europeo) della ragionevolezza, la quale dunque si conferma come clausola idonea ad intervenire nel bilanciamento di più interessi contrastanti. Si noti comunque che la misura dello sforzo imposto al responsabile deve essere valutata rispetto al risultato di portare a conoscenza dei terzi che stanno trattando i dati della richiesta dell'interessato e non, pertanto, a quello di ottenerne la cancellazione né di operarne direttamente la rimozione.

Si può infatti suggerire che in questi ultimi casi il *controller* sarebbe obbligato ad assumere un ruolo di censura attiva di contenuti che si trovano nella libera disponibilità di soggetti terzi i quali procedono ad un trattamento lecito di dati lecitamente raccolti, in quanto resi pubblici dallo stesso responsabile del

[102] Non può comunque presumersi che il trattamento avente ad oggetto o ad effetto la pubblicazione dei dati sia sempre legittimo, in quanto fondato appunto sul consenso dell'interessato o su altra ragione giustificativa: il coordinamento con il par. 1, la *ratio* della disposizione nel suo complesso e (*a contrario*) la lettera del par. 2 inducono a non escludere i casi — per il vero, com'è facile immaginare, molto frequenti — in cui il trattamento e la divulgazione pubblica sono illeciti fin dall'origine.

trattamento[103]: è naturale che il regolamento si sia dovuto attenere ad una logica di prudenza e di bilanciamento tra interessi contrastanti.

Un tentativo di calare la disposizione in ambito *cloud* non può trascurare le criticità emergenti, pur a fronte di elementi sicuramente positivi nell'ottica di una più efficace salvaguardia della posizione dell'interessato. Sebbene sia innegabile, infatti, che quest'ultimo riceva una tutela ulteriore, estesa addirittura all'impiego, secondo le circostanze del caso, di misure «anche tecniche», tuttavia, sempre nell'ipotesi in cui il cliente sia "responsabile", si intuisce che la latitudine dei mezzi tecnici in suo possesso possa non garantire[104] la capacità operativa (e, soprattutto, comunicativa, visto il contenuto dell'obbligo imposto) che al contrario verrebbe assicurata da un fornitore del servizio qualificato come *controller*[105].

Anche le risorse tecniche di quest'ultimo, comunque, potrebbero rivelarsi insufficienti, e la riflessione andrebbe estesa *a fortiori* alla figura del cliente: per definizione, il fatto che il trattamento abbia reso pubblici i dati complica notevolmente, fino a impedire del tutto, l'identificazione dei terzi[106] che vi abbiano avuto accesso e, soprattutto, li abbiano raccolti e memorizzati sui propri *server*.

Infine, si può facilmente rilevare come la disposizione taccia[107] in ordine all'eventualità che i terzi, una volta informati dal responsabile o comunque venuti a conoscenza della richiesta dell'interessato, non procedano alla cancellazione delle copie dei dati o dei *link* ad essi e, alla pari, neppure si astengano da ulteriori diffusioni dei medesimi[108]. Per contrastare queste evenienze si può ipotizzare una soluzione, di incerta realizzazione sul piano pratico. Si parta dall'assunto che la *ratio* sottostante al par. 2 considera il *controller* nella posizione più adatta (forse proprio per la presumibile maggiore disponibilità di mezzi tecnici) per rendere effettiva la richiesta dell'interessato, anche tramite, appunto, l'identificazione di altri

---

103 In realtà permane il dubbio: la diffusione di un dato e la sua disponibilità pubblica equivale alla prestazione del consenso al suo trattamento? Individua un solido orientamento contrario, almeno nelle ipotesi di utilizzo arbitrario dell'informazione, G. D'ACQUISTO, *Diritto all'oblio: tra tecnologia e diritto*, cit., p. 104.

104 Cfr. Art. 29 WP, *Parere 1/2012 sulle proposte di riforma in materia di protezione dei dati*, WP191, adottato il 23 marzo 2012, p. 14.

105 A tale proposito, per riprendere il ragionamento svolto precedentemente in nota, vale la pena di notare come il par. 2 si riempie invece di significato se se ne immagina un'applicazione ai servizi di *social network*, nei quali appunto il prestatore del servizio potrebbe a ragione rivestire il ruolo di responsabile del trattamento, con un'efficacia ben maggiore in termini di tutela dell'interessato (spesso identificabile anche con il cliente stesso): evidentemente ciò avrebbe ricadute sul contenuto del termini di servizio (alcuni dei quali, come nel caso di *Facebook*, già prevedono particolari clausole in tal senso) che gli utenti dovrebbero accettare per usufruire dell'interfaccia *online* e richiederebbe un raccordo con il regime di responsabilità previsto dalla direttiva 2000/31/CE. Per queste ultime riflessioni si veda l'approfondimento di S. SCALZINI, *I servizi di* online social network, cit., pp. 2578 ss.

106 Nella generale confusione, teorica e giurisprudenziale, dei ruoli giuridici degli attori della società dell'informazione e in assenza di pronunce sul tema, interessante lo spunto, per quanto fugace, in *AG's Opinion* C-131/12, cit., par. 110, ultimo periodo: «[Art. 17, par. 2] *seems to consider internet search engine service providers more as third parties than as controllers in their own right*».

107 Annotazione condivisa in Art. 29 WP, *Parere 1/2012*, cit., pp. 14-15: «Occorrerebbe chiarire il ruolo dei terzi che trattano dati, per definire a quali condizioni e con quale capacità possono dar seguito alla richiesta dell'interessato, nonché le eventuali conseguenze della mancata osservanza di tale richiesta».

108 La previsione finale del par. 2, fin qui trascurata, in base alla quale «se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto responsabile di tale pubblicazione», ha probabilmente più un valore (ma l'ipotesi è azzardata, in assenza di alcun tipo di conferma) di coordinamento con il principio di esenzione da responsabilità per il *controller-provider* nel caso in cui non vi sia "conoscenza effettiva" dell'illiceità dell'attività o dell'informazione, sancito dalla dir. 2000/31 (di cui v. spec. considerando n. 42): nel quadro delineato dalla proposta di regolamento, tale "conoscenza qualificata" sarebbe integrata proprio dal comportamento del responsabile del trattamento che «ha autorizzato un terzo a pubblicare dati personali».

soggetti estranei al rapporto originario che pure siano entrati in contatto con i dati. Nel caso in cui costoro non dessero seguito alla comunicazione da parte del *controller*, non può escludersi che, in una fase successiva, l'interessato stesso, dopo aver appreso dal responsabile del trattamento l'identità dei terzi ovvero dopo averli identificati con mezzi propri, si possa rivolgere loro avvalendosi del diritto riconosciutogli al par. 1[109]. L'itinerario logico si riduce alla possibilità di considerare i terzi come responsabili del trattamento[110]: in caso di risposta affermativa, essi sarebbero tenuti a dare seguito alla richiesta di cancellazione, la quale risulterebbe allora indubbiamente fondata su uno dei motivi di cui alle lettere da a) a d).

VI. OSTACOLI MATERIALI ALLA CANCELLAZIONE E TENDENZA A PREDISPORRE UN SISTEMA DI PROTEZIONE ANTICIPATA DEI DATI

Giunti a questo punto della trattazione, non si può ignorare la persistenza di alcuni interrogativi problematici che riguardano le situazioni sopra descritte e altre non ancora considerate, ma che potranno comunque rilevare in seguito. Anche le soluzioni trovate, inoltre, spesso possono risultare insufficienti: nel tentativo di ipotizzare un'applicazione del diritto alla cancellazione alla realtà informatica, infatti, emergono ulteriori aspetti critici strettamente connessi alle caratteristiche specifiche dei servizi di *cloud computing* e in parte, del *Web* 2.0, i quali possono riassumersi in due principali ordini di problemi, già segnalati in precedenza.

Il primo ha carattere essenzialmente tecnico e concerne le possibilità di dare piena soddisfazione alla richiesta dell'interessato pervenendo ad una totale cancellazione dei dati: è evidente come in tale operazione gli aspetti relativi all'evoluzione tecnologica incidano in misura notevole sull'effettività del diritto all'oblio riconosciuto dalla proposta di regolamento[111].

I fattori che determinano la perdita da parte del cliente ovvero dell'interessato stesso del controllo sui dati personali costituiscono, nella fase della cancellazione, come più volte accennato, un ostacolo all'individuazione delle numerose copie e dei *link* che sono stati peraltro creati proprio ai fini di consentire all'utente una migliore esperienza dell'interfaccia *cloud*. In particolar modo, la conservazione dei dati in *server* delocalizzati e la "condivisione" delle risorse in remoto, intesa sia dal punto di vista

[109] Potenziale soluzione che pare condivisa anche da ART. 29 WP, *Parere 1/2012*, cit., p. 15.
[110] Si veda ancora il rilievo critico in ART. 29 WP, *Parere 1/2012*, cit., p. 14: «nessuna disposizione del regolamento sembra rendere obbligatorio per i terzi rispettare la richiesta dell'interessato, salvo che non siano essi stessi considerati responsabili del trattamento».
[111] Su alcuni espedienti tecnico-informatici a tutela dei dati personali in prospettiva di una cancellazione o, comunque, di una sottrazione alla reperibilità pubblica dei dati v. G. D'ACQUISTO, *Diritto all'oblio: tra tecnologia e diritto*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, cit., pp. 103-118.

della presenza di informazioni relative a più utenti[112] sia da quello dell'impiego delle medesime in attività di diversa natura offerte sempre dal prestatore del servizio, sono caratteristiche destinate a stridere[113] con il principio per cui «occorre garantire che in ciascun caso [i dati personali] siano cancellati in modo irrecuperabile», comprendendo anche «versioni precedenti, *file* temporanei e persino frammenti di *file*»[114].

Sotto questo profilo, l'interpretazione in senso stretto del significato della "cancellazione" renderebbe praticamente impossibile la medesima in un sistema aperto quale il mondo della società dell'informazione[115]: il par. 2 dell'art. 17 risulterebbe inadeguato già laddove prevede che il *controller* contatti i terzi che stiano trattando copie dei dati rilevanti. La questione è in parte diversa per i sistemi di tipo chiuso, vale a dire accessibili ad un numero limitato di utenti, poiché in questi casi non mancherebbero i mezzi tecnici per garantire la rimozione, anche totale, delle informazioni, o comunque per procedere all'identificazione di tutti i soggetti che entrano in contatto con i dati: sulla scorta di questo esempio, una strada percorribile potrebbe consistere nello spostare la tutela ad una fase precedente, così da predisporre, per quanto possibile, un sistema (in origine) tecnicamente adeguato dal punto di vista della sicurezza e della tutela dei dati e idoneo all'applicazione dell'art. 17, par. 1.

In questa ottica si apprezza l'art. 23 della proposta di regolamento, il quale, dopo aver ribadito l'obbligo per il responsabile del trattamento di assicurare la conformità al regolamento delle operazioni cui sono sottoposti i dati, al par. 2 prevede che lo stesso responsabile «mette in atto meccanismi per garantire che siano trattati, di *default*, solo i dati personali necessari per ciascuna finalità del trattamento [e] che, di *default*, non siano resi accessibili dati personali a un numero indefinito di persone».

Le ricadute sull'esercizio del diritto all'oblio in rete sono evidenti: nonostante l'adozione di una politica di *privacy by default* non elimini il pericolo di copie fuori controllo, è cruciale che, almeno nella prima fase di utilizzo del servizio, quando ancora non ha compiuto alcuna scelta e non ha acquisito familiarità con le potenzialità (e i rischi) dell'interfaccia, l'utente sia automaticamente garantito con la forma più alta di tutela. Soltanto in un secondo momento, attraverso specifiche scelte consapevoli, egli potrà determinare liberamente quali informazioni condividere con un numero più o meno ampio di soggetti,

---

112 Si tratta della c.d. *multi-tenancy* («*sharing of resources on the provider's side*»): cfr. L. BADGER ET AL., *Cloud computing*, cit., par. 8.5.4.

113 Cfr. EUROPEAN NETWORK AND INFORMATION AGENCY (ENISA), *Cloud computing. Benefits, risks and recommendations for information security*, November 2009, (reperibile presso http://www.enisa.europa.eu), p. 10.

114 ART. 29 WP, *Parere 5/2012*, cit., par. 3.4.1.3, dove si specifica: «La cancellazione sicura dei dati personali impone che i servizi di memorizzazione vengano distrutti o smagnetizzati o che i dati personali conservati siano effettivamente cancellati mediante sovrascrittura». Il riferimento ai *file* temporanei andrebbe letto con il supporto dell'approfondimento di ART. 29 WP, *Parere 4/2012 relativo all'esenzione dal consenso per l'uso di* cookie, adottato il 7 giugno 2012.

115 Si veda ENISA, *The right to be forgotten – between expectations and practice*, pubblicato il 20 novembre 2012, reperibile dall'indirizzo http://www.enisa.europa.eu. Lo studio citato fornisce una chiara distinzione tra «*closed systems*» and «*open systems*» e, sulla scorta di osservazioni sia tecniche sia più eminentemente empiriche, giunge alla conclusione che, in ogni caso, è impossibile impedire del tutto la copia non autorizzata di dati che siano resi accessibili al pubblico e una successiva disseminazione di tali dati, con la perdita della certezza assoluta in merito alle possibilità di cancellazione.

auspicabilmente conosciuti o quantomeno affidabili, agendo sulle "impostazioni della *privacy*", strumento di regolazione del livello di esclusione del pubblico dall'accesso ai dati.

L'utente potrà così controllare con maggiore accuratezza la diffusione dei contenuti che egli immette *online*, identificando i destinatari una volta per tutte o anche in relazione ad ogni singolo dato, il quale diventa più facilmente tracciabile. Infatti, al momento della richiesta di cancellazione da parte dell'interessato il responsabile del trattamento, sia che coincida con il cliente (il quale pure può essere interessato, a seconda dei dati coinvolti) sia che si identifichi con il fornitore, potrà fare riferimento ad un preciso elenco di soggetti previamente selezionati tramite le impostazioni apposite: con questo accorgimento, il quale comunque non tutela da *download*, archiviazione e nuova circolazione delle informazioni, è plausibile immaginare un migliore funzionamento dell'art. 17, par. 2, in quanto i terzi dovrebbero risultare sempre determinabili e raggiungibili e, nel caso in cui siano stati correttamente selezionati, dovrebbero fornire adeguata garanzia dell'esecuzione della richiesta di cancellazione.

In ambito di *cloud computing* una simile disposizione troverà pertanto applicazione su due profili connessi: da un lato, il cliente-*controller* avrà l'obbligo di scegliere con cura sia il fornitore del servizio di cui intende avvalersi sia la platea dei destinatari o dei soggetti a cui sono rese accessibili le informazioni, affinché il sistema nel suo complesso risulti il più adatto ad assicurare la protezione dei dati; dall'altro, il *provider* (soprattutto nel caso in cui sia considerato responsabile o co-responsabile del trattamento) dovrà mettere in atto misure organizzative e, specialmente, tecniche, affinché i termini d'uso e le condizioni concrete di funzionamento del sistema prevedano un livello iniziale massimo di chiusura all'esterno e la possibilità per l'utente di modificare in ogni momento le proprie preferenze sulla *privacy*[116].

VI.1. PER UNA RIVALUTAZIONE DEL PRINCIPIO DI NECESSITÀ NEL TRATTAMENTO DEI DATI

Come ultimo spunto sul tema, si segnala che proprio in tema di diritto alla cancellazione, e proprio con riferimento a servizi in rete come quelli di tipo *cloud*, potrebbe essere rivalutato, quale strumento alternativo di tutela anticipata, il principio di necessità sancito nella disciplina italiana dall'art. 3 del d. lgs. 196/2003[117].

[116] *Cfr* ART. 29 WP, *Parere 5/2009*, cit., parr. 3.1.2 e 3.2: riflessioni coerenti anche con una lettura di tipo sostanziale dell'art. 30, par. 2, della proposta di regolamento.

[117] Conviene riportarne il testo: «I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettono di identificare l'interessato solo in caso di necessità».

La scelta del legislatore nazionale di innovare (ancora una volta) rispetto alla direttiva comunitaria esprime una chiara comprensione delle dinamiche evolutive dei servizi della società dell'informazione e rappresenta il tentativo di ridurre il divario che separa tradizionalmente la dimensione normativa dall'incessante mutare della realtà dei fatti da regolare: la serietà degli intenti è confermata dalla collocazione della disposizione in apertura del Codice, insieme ai principi cardine dell'intera materia, ai quali appunto si affianca nella funzione di definire una «politica del diritto particolarmente impegnativa»[118] caratterizzata da un «ampio approccio di tutela sostanziale [offerto] anche in via preventiva»[119].

È naturale avvertire il problema del coordinamento di questo principio con le regole generali di pertinenza e di non eccedenza dei dati, riconducibili a loro volta al principio di finalità: in un'ottica di economia degli strumenti normativi, l'ambito di autonoma applicazione del principio di necessità potrebbe essere individuato nella configurazione dell'ambiente in cui i dati sono trattati[120] e, in ossequio alla natura precauzionale che gli è riconosciuta, nella valutazione *a priori* dell'idoneità del trattamento a raggiungere lo scopo prefissato[121].

Tuttavia, accettandone una simile lettura fondata sulla ricerca di un equilibrio nella dialettica tra fini e mezzi, si può dubitare dell'efficacia della risposta offerta dal giudizio in base al principio di necessità in tutti i casi in cui il servizio della società dell'informazione ha uno scopo tanto indeterminato, ovvero comunque determinabile mediante criteri tanto aleatori, che la finalità pare quasi coincidere proprio con quello che, di consueto, è il mezzo impiegato, ossia il trattamento stesso.

Ad esempio, si scorge con difficoltà come garantire il rispetto del principio di finalità da parte di quei *cloud provider* i quali, non limitandosi ad attività di semplice *storage*, si distinguono proprio per l'agevolazione e la promozione dinamica delle relazioni sociali degli utenti: la volontà stessa di questi ultimi, seppure all'interno di certi limiti, è orientata nel senso di ottenere una riproduzione della vita quotidiana, soprattutto nelle sue caratteristiche (forse ideali, ma non per questo meno agognate) di casualità e novità, le quali possono essere assicurate da meccanismi quali continui suggerimenti di condivisione, interazioni inaspettate, casuali incroci con commenti, fotografie e informazioni altrui.

In quest'ottica il principio di necessità risulta svuotato di significato, poiché in alcuni casi, paradossalmente, costituisce un ostacolo al perseguimento dei risultati in vista dei quali si utilizza il servizio; in più, la sempre maggiore integrazione tra sistemi informatici e il crescente affidamento nelle applicazioni *online*, aspetti tipici del fenomeno *cloud computing*, non ne pregiudicheranno la vitalità solo

118 S. RODOTÀ, *Europa e dir. priv.*, 2004, p. 6.
119 G. BUTTARELLI, *Commento all'art. 3*, in C. M. BIANCA – F. D. BUSNELLI (a cura di), *Commentario al D. Lgs. 30 giugno 2003, n. 196*, cit., p. 33.
120 *Ibidem*, p. 34.
121 R. D'ORAZIO, *Il principio di necessità nel trattamento dei dati personali*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Giappichelli, 2007, pp. 21-22.

laddove se ne proponga un'interpretazione "tecnologicamente orientata", compatibile con le recenti e future evoluzioni del mondo di Internet[122].

Una strada per restituire attualità all'art. 3 potrebbe consistere nell'intenderlo come un archetipo delle attuali teorie di *privacy by default* e, soprattutto, *privacy by design*, capace di inserire la prescrizione di un trattamento "minimalista" dei dati in una prospettiva di tutela di vasto respiro, saldamente radicata nella realtà tecnica ed aperta alle integrazioni derivanti dai principi generali che regolano la materia: in questo modo, peraltro, sarebbe dimostrata la lungimiranza e la sapiente tecnica normativa del legislatore nazionale, la cui opera sembra aver precorso i tempi, anticipando le più recenti novità a livello europeo.

VII. A PROPOSITO DEI LIMITI GIURIDICI: LA COMPLESSITÀ DI UN BILANCIAMENTO IN CONCRETO TRA GLI INTERESSI RILEVANTI

VII.1. INDICI INTERPRETATIVI E SPUNTI RICOSTRUTTIVI DESUMIBILI DALLA GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA

Come segnalato, il secondo problema relativo all'esecuzione del diritto dell'interessato alla cancellazione è strettamente collegato al primo, di cui riprende la questione di fondo, ma in una prospettiva diversa, vale a dire quella della fattibilità giuridica.

Se la rimozione materiale delle informazioni incontra una serie di gravi ostacoli sul piano tecnico, tanto da suggerire una conclusione nel senso dell'impossibilità di una sua completa realizzazione, restano da valutare tutti gli aspetti di diritto che si coagulano attorno ad essa: a richiedere un ulteriore scrutinio non è pertanto l'ammissibilità astratta del diritto alla cancellazione, ma la sua corretta definizione, a sua volta da ricercarsi mediante l'analisi dei limiti che lo stesso incontrerebbe. Limiti che, appunto, non consistono più soltanto nella praticabilità concreta delle misure che andrebbero a colpire le informazioni o copie di esse, bensì nelle situazioni giuridiche connesse ai dati ovvero facenti capo ai soggetti che con i dati siano venuti a contatto a diverso titolo.

Identificare i terzi che procedono al trattamento, recuperare e distruggere i dati in loro possesso sono attività che, pur rappresentando esercizio di un diritto previsto dal legislatore stesso, possono confliggere con i diritti di cui siano titolari altri soggetti, e rendono pertanto necessario un bilanciamento da parte degli operatori in sede di applicazione. Come ovvio, non si ravvisano precedenti

[122] Si propone qui una nota assai suggestiva: già al momento dell'entrata in vigore della normativa italiana di trasposizione si sottolineava come le nuove regole costituissero risposta a particolari esigenze del mondo dell'informatica, tra cui, in particolare l'utilizzo di «p.c. mediante software aggiornati automaticamente in rete oppure dislocati in remoto e utilizzati tramite connessione, "in affitto" a tempo» (G. BUTTARELLI, *Commento all'art. 3*, cit., p. 33). La lungimiranza di tale acuta osservazione sembra innegabile ove vi si legga il riferimento ad un rudimentale archetipo di un modello di funzionamento di tipo *cloud*.

in materia in sede di Unione europea, ma è forse possibile scovare nella giurisprudenza della Corte di giustizia delle direttrici interpretative suscettibili di un'estensione prospettica al fenomeno del c*loud computing*, almeno per quelle numerose caratteristiche che esso condivide con il mondo ICT.

In ambito informatico la Corte di Lussemburgo[123] fissa un chiaro limite all'imposizione di un obbligo in capo ai prestatori di servizi della società dell'informazione, in particolare gli ISP. S senza poter ripercorrere integralmente il panorama giuridico in cui si cala tale orientamento giurisprudenziale[124], è importante ricordare che, in tema di violazione del diritto d'autore, i giudici stabiliscono che il diritto comunitario osta all'ingiunzione ad un prestatore di servizi di *hosting*[125] di predisporre un sistema di filtraggio, a titolo preventivo e senza limiti di tempo, delle informazioni memorizzate sui *server* di detto prestatore dagli utenti dei suoi servizi.

Il meccanismo di filtraggio così realizzato comporterebbe per il fornitore, tra le altre, un'attività di sorveglianza generalizzata delle informazioni dal medesimo memorizzate, che riguarderebbe sia la quasi totalità dei dati sia ciascuno degli utenti dei servizi di tale prestatore[126]: da questo scenario ipotetico la Corte trae due conclusioni.

In primo luogo, sarebbe messa a repentaglio la riservatezza degli utenti e dunque verrebbe pregiudicato il necessario «*fair balance*»[127] tra protezione del *copyright*, parte del diritto fondamentale di proprietà, e protezione dei diritti fondamentali della persona[128]; tale rilievo non appare idoneo ad influire in questa sede di analisi, in quanto si prescinde dalle problematiche relative all'esistenza di diritti di proprietà intellettuale, e non è certo in nome di questi ultimi che potrebbe individuarsi un limite alla piena tutela della *privacy* dell'utente di servizi *cloud*. Piuttosto, si presenterebbe la situazione in cui il diritto alla riservatezza dei clienti del medesimo fornitore ovvero di soggetti terzi allo stesso collegati deve essere bilanciato con l'invocazione che un altro soggetto abbia fatto del proprio diritto alla cancellazione, il quale, in ipotesi, può essere soddisfatto materialmente soltanto attraverso la predisposizione di un sistema di monitoraggio e di tracciamento degli accessi e delle operazioni che riguardano i dati, in modo da agevolare la successiva ed eventuale rimozione di questi ultimi: nel caso in cui il sistema si applichi a titolo preventivo, indistintamente nei confronti di tutti gli utenti e senza limiti di tempo —

123 Il riferimento è a due pronunce, ravvicinate nel tempo, entrambi su ricorso in via pregiudiziale e nell'ambito di procedimenti instaurati dalla società belga SABAM: Corte di giustizia UE, 24 novembre 2011, C-70/10, *Scarlet Extended c. SABAM*, in Racc., 2011, I-11950 e Corte di giustizia UE, 16 febbraio 2012, C-360/10, *SABAM c. Netlog*, in *http://curia.europa.eu*, con nota unica di M. COLANGELO, *Internet e sistemi di filtraggio tra* enforcement *del diritto d'autore e tutela dei diritti fondamentali: un commento ai casi* Scarlet *e* Netlog, in *Nuova giur. civ. comm.*, 2012, 7-8, p. 580.

124 Per i dovuti approfondimenti si rimanda a M. SIANO, *La sentenza* Scarlet *della Corte di Giustizia: punti fermi e problemi aperti*, in F. PIZZETTI (a cura di), *I diritti nella "rete" della rete. Il caso del diritto di autore*, Giappichelli, 2012, p. 81.

125 Si noti che *Netlog*, uno dei *provider* coinvolti, svolge le funzioni di un *social network*: dovrebbero tornare alla mente le riflessioni svolte in merito ai problemi di qualificazione giuridica di questi soggetti.

126 Cfr. sentenza *Netlog*, cit., par. 37 e sentenza *Scarlet Extended*, cit., par. 39.

127 Sentenza *Netlog*, cit., par. 47.

128 In particolare, i diritti fondamentali alla tutela dei dati personali e alla libertà di ricevere o di comunicare informazioni, entrambi tutelati dalla Carta dei diritti fondamentali dell'Unione europea, rispettivamente agli artt. 8 e 11: v. sentenza *Netlog*, cit., par. 48.

caratteristiche probabilmente necessarie per assicurare una effettiva fattibilità tecnica della cancellazione delle informazioni — non vi è ragione per credere che la Corte di Lussemburgo abbandoni la posizione di recente assunta, operazione che, a giudicare dai diritti in gioco, richiederebbe un complessa ed articolata motivazione, probabilmente inseparabile dalle circostanze del caso concreto.

Altrettanto interessante il secondo argomento contrario all'imposizione di un obbligo di controllo generalizzato in capo al del *provider*, sempre improntato alla tecnica del bilanciamento tra diritti: l'ingiunzione a predisporre un sistema di filtraggio avrebbe conseguenze negative non limitate ai soli utenti del servizio, ma causerebbe una «grave violazione della libertà di impresa»[129], poiché obbligherebbe il fornitore a predisporre un sistema informatico complesso, costoso e permanente, unicamente a sue spese.

È evidente che le fattispecie in esame, ossia quella prospettata nel caso sottoposto alla cognizione della Corte di giustizia e quella ipotizzabile in ambito di *cloud computing*, sono divergenti: se nel primo caso il richiamo alla libertà di impresa, motivato dalla necessità di evitare un freno ingiustificato all'attività degli operatori del settore, assume di fatto un ruolo sinergico rispetto al diritto alla protezione dei dati personali al fine di garantire la tutela della riservatezza degli utenti, nel secondo, in senso inverso, si immagina di dare rilevanza all'eccessiva onerosità economica dell'obbligo gravante sul prestatore del servizio così da negare una salvaguardia indiscriminata ed assoluta all'interesse giuridicamente qualificato del soggetto alla totale rimozione delle informazioni che lo riguardano, la quale dovrebbe essere attuata mediante l'impiego di dispendiosi mezzi tecnici.

Tuttavia, non può essere escluso *a priori* che si presenti l'esigenza di operare un bilanciamento o una comparazione tra diritti in cui libertà d'impresa e tutela della *privacy* non si collocano sullo stesso versante, in contrapposizione ai diritti di proprietà intellettuale, bensì, in ipotesi di irrilevanza di questi ultimi, si fronteggiano limitandosi a vicenda.

Una simile lettura, per quanto in contrasto apparente con la pronuncia richiamata — alla quale comunque può accostarsi, come visto, a seguito di un oculato *distinguishing* che sottolinei le differenze tra i fatti del caso — risulta avvalorata da ulteriori indici ravvisabili nella giurisprudenza della stessa Corte di giustizia.

Nell'ambito del diritto dell'Unione europea, infatti, deve riaffermarsi l'importanza primaria della libertà d'impresa e dei principi a cui essa si ricollega, tanto più in considerazione del fatto che l'attività di rimozione di informazioni potrebbe comportare verosimilmente, per la struttura della rete stessa, un ingente dispendio di risorse economiche. La posizione della Corte di Lussemburgo in materia non può

[129] Sentenza *Netlog*, cit., par. 46 e sentenza *Scarlet Extended*, cit., par. 48.

essere trascurata[130]: si registra la tendenza a considerare i diritti economici in posizione paritetica rispetto ai diritti della persona e una serie di riferimenti normativi internazionali di stampo convenzionale presuppongono la riconduzione di entrambi le tipologie alla categoria dei diritti fondamentali dell'uomo[131].

Una tale visione, pienamente rispondente alla logica del mercato unico, potrebbe al pari riflettersi in ambito di valutazione dei presupposti richiesti dall'art. 17 per l'esercizio del diritto alla cancellazione: a maggior ragione, in occasione delle prime pronunce e laddove si consideri che lo stesso diritto, per quanto logicamente attinente alla sfera relativa alla tutela del trattamento dei dati personali e dell'identità personale, è controverso nei contorni essenziali e non consta aver ricevuto una piena investitura come diritto fondamentale, almeno a livello di corti dell'Unione.

D'altra parte, a ben guardare, se non vi è chiarezza in merito alla portata concreta del contenuto che il "diritto all'oblio" potrebbe assumere, come si è tentato di evidenziare, anche i contorni ed una univoca classificazione dello stesso rimangono elusivi.

Peraltro è interessante notare che la possibilità di estendere il ragionamento della Corte di giustizia al *cloud computing* risulta avvalorata dalle già menzionate conclusioni del Gruppo di lavoro Art. 29, secondo la cui prospettiva il *cloud provider* si qualifica principalmente come prestatore di un servizio di (mero) *hosting*, tanto da essere identificato, nell'ambito della disciplina sulla protezione dei dati personali, come incaricato del trattamento, data la sua tendenziale passività, e non come *controller*, figura a cui si associa, come visto, un ruolo non puramente esecutivo di scelte altrui.

Resterebbe comunque da chiarire il rapporto con l'art. 17 della proposta di regolamento, il quale prevede appunto l'imposizione di un obbligo di dare esecuzione alla richiesta dell'interessato in capo al responsabile del trattamento, lo stesso soggetto che, ai sensi del par. 2, sarebbe l'unico tenuto ad attivarsi presso i terzi con apposita comunicazione proprio attraverso «misure ragionevoli, anche tecniche», al cui impiego possono riconnettersi le riflessioni svolte sulla scia della giurisprudenza europea. Tuttavia, stante la necessità di operare un bilanciamento tra situazioni giuridiche attinenti a diritti della persona, non si può indubbiamente trascurare l'eventualità che esigenze di tutela della riservatezza degli utenti del servizio e dei terzi in generale emergano anche nei casi in cui a condurre le operazioni di rimozione ovvero a predisporre invasive misure preventive di monitoraggio sia il singolo cliente *cloud*, nel ruolo appunto di responsabile, dal quale non vi è motivo per pretendere un livello inferiore di rispetto di diritti fondamentali, quale il diritto alla riservatezza.

---

130 M. JAEGER, *Il diritto di proprietà quale diritto fondamentale nella giurisprudenza della Corte di giustizia*, in Europa e dir. priv., 2011, 2, p. 349.
131 Il tema, vastissimo, è ben inquadrato da C. SALVI, *Libertà economiche, funzione sociale e diritti personali e sociali tra diritto europeo e diritti nazionali*, in *Europa e dir. priv.*, 2011, 2, p. 437.

VII.2. LA LIBERTÀ DI ESPRESSIONE COME ANTAGONISTA NATURALE DEL DIRITTO ALLA CANCELLAZIONE (CENNI)

Invero, quanto detto, con particolare riferimento al diritto alla riservatezza di soggetti terzi e alla libertà d'impresa dei soggetti prestatori di servizi su Internet, è servito ad individuare potenziali limiti giuridici (e non di fatto) all'esercizio concreto del diritto all'oblio, la cui piena applicazione pratica rischia di confliggere, a causa dell'ampiezza e della pervasività delle misure tecniche, con i diritti fondamentali di cui soggetti terzi sono titolari in situazioni strettamente connesse all'esecuzione di dette misure.

Il tema del "diritto all'oblio", tuttavia, racchiude il germe di un contrasto intrinseco con un altro diritto fondamentale che può essere prefigurato già a livello astratto, in sede di inquadramento sistematico dello stesso diritto alla cancellazione: il diritto alla libertà di espressione, la cui particolare rilevanza, ancor più avvertita nella società dell'informazione, lo rende indubbiamente valido antagonista della tutela della riservatezza nelle situazioni in cui la volontà dell'interessato di elidere informazioni personali condurrebbe al probabile risultato di bloccare comunicazioni lecite dotate di particolari caratteri qualificanti[132].

Per chiari motivi, lo studio delle possibili vie di soluzione dell'antinomia, nonché un inquadramento delle posizioni in gioco nella costellazione dei diritti fondamentali della persona, per quanto temi di indubbia attualità, non potrà qui ricevere uno spazio adeguato, ma, una volta che ne siano stati individuati alcuni tratti salienti e spunti di particolare significato per la questione in esame, potrà fornire un valido apporto critico alle successive riflessioni di questo contributo che si avvia alla conclusione.

La necessità di operare un bilanciamento con la libertà di espressione fornisce innanzitutto risposta all'inevitabile interrogativo che sorge in seguito alla considerazione per cui, nel disegno complessivo dell'art. 17, a voler prescindere dalle criticità sia pratiche sia giuridiche messe in luce, dunque al di là degli ostacoli alla realizzazione della pretesa, il diritto riconosciuto sia fin troppo vasto[133].

La disposizione medesima prevede, tra le deroghe all'obbligo di eseguire la richiesta di cancellazione, il caso in cui «conservare i dati personali […] sia necessario: a) per l'esercizio del diritto alla libertà di espressione in conformità dell'articolo 80» (par. 3). Il testo non fornisce indicazioni sufficienti per meglio comprendere gli elementi da tenere in considerazione ai fini del contemperamento tra diritti, e le incertezze aumentano a leggere il contenuto del rinvio, il quale stabilisce la competenza dei singoli Stati

---

132 Si tratta dei parametri di pertinenza, verità e continenza, elaborati dalla giurisprudenza a partire dalla fondamentale Cass. civ., sez. I, 18 ottobre 1984, n. 5259, in *Foro it.*, 1984, I, c. 2711, con nota di R. PARDOLESI: si veda anche M. R. MORELLI, *Oblio (Diritto all')*, in *Enc. dir.*, *Agg.*, Vol. VI, Giuffrè, 2002, p. 853.

133 Le osservazioni più scettiche e critiche giungono dagli Stati Uniti, dove, come noto, la concezione della libertà di espressione è particolarmente forte: con toni di seria preoccupazione J. ROSEN, *The Right to Be Forgotten*, in *64 Stan. L. Rev. Online 88*, 13 febbraio 2012, p. 88 («*[the right to be forgotten] represents the biggest threat to free speech on the Internet in the coming decade*»);

membri in materia di deroghe ed esenzioni rispetto alla disciplina del regolamento nei casi di trattamento effettuato «esclusivamente a scopi giornalistici o di espressione artistica o letteraria». Anche ove dai primi due commi dell'art. 17 si ricavasse (come d'altra parte è auspicabile) una tutela uniforme e coerente a livello europeo, su questa incomberebbe comunque la frammentarietà del quadro risultante dalle eccezioni decise dagli Stati e il regime applicabile in concreto presenterebbe forti tratti di disomogeneità su base territoriale[134].

D'altra parte, conviene accennare il rilievo che la libertà di manifestazione del pensiero assume nelle dinamiche della società virtuale, la quale ne favorisce l'esercizio senza filtri e in forma diffusa[135]: se le nuove tecnologie dilatano a dismisura le capacità di ciascun utente di entrare in contatto con l'esterno, rendendo possibile trasmettere e ricevere informazioni e contenuti multimediali di vario genere, Internet diviene uno dei terreni principali su cui valutare la consistenza delle misure normative a tutela di un diritto fondamentale come quello in questione[136].

SEZIONE IV

SPAZI E LIMITI DELL'APPROCCIO TRADIZIONALE AL FENOMENO: L'ESPERIENZA ITALIANA

VIII. LA DIVERSA LETTURA NAZIONALE DEL DIRITTO ALL'OBLIO

Allo stesso tempo, il diritto alla libertà di espressione può venire in risalto come parametro sulla base del quel giustificare un'ipotetica diversità di disciplina per i casi in cui l'interessato abbia direttamente immesso su Internet dati personali e per quelli, ben distinti, in cui un terzo abbia reso pubblici i medesimi avvalendosi di un elemento di legittimazione diverso dal consenso[137].

La precisazione è tutt'altro che irrilevante, sia in ambito di diritto alla cancellazione sia nel contesto delle tecnologie informatiche.

134 Cfr. K. LARSEN, *Europe's "Right to Be Forgotten" Regulation May Restrict Free Speech*, Newsletter of the ABA Litigation Section's First Amendment & Media Litigation Committee (Fall 2012/Winter 2013), reperibile a partire dall'indirizzo http://www.lskslaw.com.

135 Nell'ambito della riflessione relativa anche al diritto all'oblio si veda *AG's Opinion* C-131/12, cit., parr. 120-122, dove si richiama la tutela garantita, con particolare attenzione alle informazioni *online*, dall'art. 11 della Carta dei diritti fondamentali dell'Unione europea («[il diritto alla libertà di espressione] include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee […]».

136 D. MULA, *Libertà di manifestazione del pensiero in rete*, in G. CASSANO – G. VACIAGO – G. SCORZA (a cura di), *Diritto dell'Internet*, cit., pp. 7 ss.

137 Un fondamento giuridico è comunque imprescindibile perché il trattamento non sia radicalmente illegittimo: in tali casi, sul piano delle conseguenze, non vi sarebbe alcun ostacolo (di diritto) alla cancellazione delle informazioni.

Sotto il primo profilo, è il momento di ricordare come, in realtà, nella giurisprudenza e nella dottrina italiana[138] si parli propriamente e solitamente di "diritto all'oblio" quando l'iniziale diffusione delle informazioni personali non è avvenuta su base consensuale né in modo volontario per opera diretta dell'interessato, ma in risposta ad un interesse pubblico alla conoscenza delle stesse: vengono appunto in rilievo quelle fattispecie in cui un soggetto pretende che dati o eventi passati, in origine legittimamente resi pubblici[139], non siano rievocati attraverso una qualche forma di riproposizione, sul presupposto che, in mancanza di un nuovo reale (o serio) interesse pubblico, «il trascorrere del tempo e il mutamento delle circostanze […] la rendano illecita»[140].

In aggiunta, sotto il secondo profilo, con sempre maggiore frequenza[141], il diritto all'oblio così inteso rileva in casi in cui si tratta della trasposizione dal formato cartaceo al formato digitale degli archivi storici di testate giornalistiche[142]; si noti poi che l'archiviazione in rete potrebbe addirittura essere realizzata avvalendosi di un vero e proprio servizio di *cloud computing*, alla luce dei noti vantaggi riconnessi a questa tecnologia, tra cui spicca in proposito la possibilità di rendere le informazioni più facilmente accessibili nonché di agevolarne l'organizzazione e la consultazione mediante strumenti applicativi di vario genere.

In queste ipotesi è immediato individuare molte delle questioni fin qui affrontate, adesso riproposte in una nuova ottica e sotto una diversa luce che potrebbe consentire di dare risposta ad interrogativi rimasti ancora irrisolti[143].

Si enucleino gli elementi principali della fattispecie: una prima diffusione dei dati personali ad opera di un soggetto diverso dall'interessato, l'originaria legittimità del trattamento, fondata sul diritto di informazione e, dunque, sull'interesse pubblico alla conoscenza dei dati, la percezione, da parte dell'interessato, in riferimento ad una possibile rievocazione dell'informazione, del rischio di

---

138 Impossibile citare l'intera bibliografia sul tema: nel tentativo di restituire un quadro anche diacronico, si segnalano, tra i contributi principali all'elaborazione della riflessione giuridica sulla materia, almeno nei suoi aspetti generali, A. T. AULETTA, *Riservatezza e* droit à l'oubli, in AA. VV., *L'informazione e i diritti della persona*, Napoli, 1983, p. 129; G. B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, p. 801; G. NAPOLITANO, *Il diritto all'oblio esiste (ma non si dice)*, nota a Trib. Roma 15 maggio 1995, in *Dir. inf.*, 1996, p. 427; P. LAGHEZZA, *Il diritto all'oblio esiste (e si vede)*, nota a Cass. civ., sez. III, 9 aprile 1998, n. 3679, in *Foro it.*, 1998, I, c. 1835; M. R. MORELLI, *Oblio (Diritto all')*, cit., p. 848; S. NIGER, *Il diritto all'oblio*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, Padova, 2007, p. 59; M. MEZZANOTTE, *Il diritto all'oblio, Contributo allo studio della* privacy *storica*, Napoli, 2009.

139 Ciò vale a distinguere il diritto all'oblio dal diritto alla riservatezza: cfr. M. R. MORELLI, *Oblio (Diritto all')*, cit., p. 851.

140 A. T. AULETTA, *Riservatezza e* droit à l'oubli, cit., p. 129.

141 Cfr. GARANTE PRIVACY, *Relazione annuale 2012*, pp. 155-156.

142 Una fattispecie simile, si ricorda, ha fornito l'occasione per il rinvio pregiudiziale alla Corte di giustizia dell'Unione europea che ha dato origine alla citata causa C-131/12.

143 Il ragionamento che segue è inteso appunto a facilitare la comprensione dei limiti concettuali del "diritto all'oblio" e, di conseguenza, delle concrete prospettive di applicazione. Un buon esempio è costituito dal rapporto tra la domanda 2) e la domanda 3) di Fleischer, citate *supra*, rispettivamente «*If I post something, and someone else copies it and re-posts it on their own site, do I have the right to delete it?*» e «*If someone else post something about me, should I have a right to delete it?*»: l'elemento che distingue le due ipotesi e che importa una diversità di disciplina andrebbe ricercato non solo e non tanto nel percorso compiuto dall'informazione prima di essere divulgata in rete (sebbene alla luce di tale criterio non possa parlarsi di piena identità), bensì nel presupposto che ne legittima la pubblicazione.

conseguenze pregiudizievoli a situazioni giuridiche protette di particolare valore[144], come appunto il diritto alla *privacy*.

Lo schema applicativo classico del diritto all'oblio implica dunque un certo grado di intensità del rischio di subire un pregiudizio, il quale si considera raggiunto nei casi di rievocazione dell'informazione un tempo assurta agli onori della cronaca senza che ricorrano le condizioni (di interesse pubblico) che ne giustificherebbero una nuova diffusione[145]. Con riguardo agli archivi, la linea tenuta del Garante italiano si è mantenuta coerente nel senso di escludere che la conservazione delle informazioni nel tempo, nella forma di articoli di giornale, equivalga alla reiterata pubblicazione delle medesime: in particolare, l'interesso storico, statistico e scientifico costituisce motivo distinto rispetto alle finalità giornalistiche e dunque, anche in assenza dello specifico interesse pubblico sottostante a queste ultime, si rivela idoneo a fondare la legittimità di un trattamento successivo di dati rilevati per finalità di diverso tipo[146].

L'avvento di Internet introduce un elemento di rottura in questo scenario, poiché nel mondo della rete, a causa della rapidità dei collegamenti, della natura dei contenuti *online* e del carattere virtuale del sistema complessivo, il momento della "potenza" vive a stretto contatto con quello dell' "atto", il che significa, nel caso specifico, che il fatto che un'informazione anche solo esista, per quanto nascosta, consente di ritenere superata una immaginaria soglia di accessibilità effettiva e di serietà del rischio di una reiterata diffusione.

Il rilievo secondo il quale sarebbe apprezzabile un unico fenomeno comunicativo, limitato alla prima pubblicazione della notizia in rete, non può valere l'osservazione per cui l'originaria legittimità della medesima risulta idonea ad escludere ogni questione problematica inerente alla permanenza delle informazioni su Internet[147]. Da un punto di vista sostanziale, infatti, per quanto non si verifichi una "nuova narrazione", la diffusione dei dati *online* e la conseguente conservazione a tempo indeterminato che se ne genera attraverso la memorizzazione sotto forma di innumerevoli copie disseminate in *server* delocalizzati assumono di necessità il valore di una riproposizione ininterrotta dei dati stessi[148]: «non si

144 Su quest'ultimo punto si richiamano le parole di Cass. 3679/1998, cit., la quale intende il diritto all'oblio come «giusto interesse di ogni persona a non rimanere indeterminatamente esposta a danni ulteriori […] al suo onore e alla sua reputazione».

145 *Cfr* G. B. FERRI, *Diritto all'informazione*, cit., 813: «In tale prospettiva non c'è diversità di tutela tra la notizia mai pubblicizzata e quella che abbia avuto una pregressa e, comunque, legittima notorietà»: non è un caso che «nella selezione delle fattispecie rilevanti, la giurisprudenza [abbia] fatto ricorso agli stessi requisiti legittimanti il corretto esercizio della libertà di cronaca» (F. MANGANO, *Diritto all'oblio*, in *Giur. merito*, 2012, 12, p. 2624).

146 Provvedimenti Garante 18 marzo 2010, doc. *web* n. 1712827; 16 marzo 2010, doc. *web* n. 1734973; 21 marzo 2012, doc. *web* n. 1892254; v. anche artt. 11 e 99 d. lgs. 196/2003.

147 Così invece A. MANTELERO, *Il diritto all'oblio dalla carta stampata ad Internet*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, cit., p. 156. Anche a condividere tale impostazione, peraltro, potrebbe trovarsi diversa soluzione valorizzando il fattore temporale che contribuisce a connotare l'interesse dell'individuo all'oblio delle vicende che lo riguardano: cfr. M. R. MORELLI, *Oblio (Diritto all')*, cit., p. 851; v. anche nota seguente.

148 In tale ottica il valore del tempo potrebbe essere inteso «non già come misura dello scarto temporale tra l'interesse passato e l'interesse attuale alla notizia, bensì come durata della esposizione della notizia all'accesso generalizzato» F. MANGANO, *Diritto all'oblio*, cit., p. 2637.

tratta di un evento che si ripropone all'attenzione del pubblico, bensì di un evento che potenzialmente non è mai uscito dall'attenzione del medesimo»[149].

In sintesi, nei casi in cui l'invasione della *privacy* dell'individuo sia stata giustificata dall'esercizio del diritto alla libertà di informazione, i dati immessi in rete godono di una forma di pubblicità permanente, di intensità proporzionale rispetto al livello di interconnessione di servizi e applicazioni digitali, non accompagnata però, almeno in modo continuativo, dall'interesse pubblico che aveva legittimato il trattamento. Sotto questo aspetto, dunque, a rigor di logica, il "diritto all'oblio", piuttosto che in un divieto di rievocazione, dovrebbe concretizzarsi nella rimozione o, quantomeno, nell'oscuramento (si legga: non accessibilità) dell'informazione.

La strada della cancellazione, oltre a scontrarsi con le difficoltà segnalate in precedenza per quanto riguarda la fase applicativa, collide comunque con l'essenza dell'ipotesi in esame: è necessario ricordare come l'assenza di un interesse pubblico concomitante alla permanenza in rete dell'informazione e che possa giustificare la sua indiscriminata accessibilità non pregiudichi, in realtà, la legittimità della raccolta dei dati né la successiva diffusione, ove siano avvenute nell'ambito dell'esercizio di un altro diritto fondamentale o in presenza di altra valida giustificazione. Infatti, poiché un interesse pubblico dotato dei requisiti necessari sussisteva effettivamente al momento della pubblicazione, tale fatto non può più essere messo in discussione, e pertanto deve essere garantita l'esistenza dell'articolo nell'archivio; d'altra parte, deve riconoscersi un autonomo interesse alla conservazione delle informazioni per finalità non giornalistiche, ma di ricerca storica, anche le quali possono a loro volta costituire esercizio del diritto fondamentale alla libertà di manifestazione del pensiero[150].

Con riguardo agli archivi, in particolare, una diversa soluzione prospettabile, la quale risulta avvalorata dall'esperienza delle decisioni del Garante italiano[151], consiste nel tentativo di agire attraverso lo strumento che determina la reperibilità immediata delle informazioni, vale a dire sui motori di ricerca, affinché questi ultimi le escludano dai risultati ottenuti in corrispondenza di una precisa interrogazione che abbia ad oggetto elementi riconducibili all'informazione rispetto alla quale si invoca il diritto all'oblio[152]. Da un punto di vista applicativo, poi, l'equilibrio tra le esigenze di tutela del singolo e le finalità di ricerca storica potrebbe essere individuato nella creazione di appositi motori di ricerca interni all'archivio digitale[153], l'impiego dei quali consentirebbe di ridurre i casi di emersione casuale delle

149 G. FINOCCHIARO, *La memoria della rete*, cit., p. 397.
150 Oltre all'art. 21 Cost., tuttavia, una forma di garanzia indipendente si ritrova all'art. 9 Cost., relativo alla promozione dello sviluppo della cultura e della ricerca, e all'art. 33 Cost., in tema di creazione artistica e ricerca scientifica.
151 Provvedimenti 12 aprile 2012, doc. *web* n. 1894581; 19 luglio 2012, doc. *web* n. 2065905; 4 ottobre 2012, doc. *web* n. 2104293; 18 ottobre 2012, doc. *web* n. 2130029.
152 L. FEROLA, *Dal diritto all'oblio al diritto alla memoria sul* Web. *L'esperienza applicativa italiana*, in *Dir. inf.*, 2012, 6, 1016-1017.
153 A. MANTELERO, *Il diritto all'oblio dalla carta stampata ad Internet*, cit., p. 162.

informazioni e di limitare le vie di accesso alle medesime senza escludere che queste siano raggiungibili liberamente a chi sia mosso da intenzioni comunque compatibili con il diritto all'informazione[154].

IX. IL CASO DEGLI ARCHIVI GIORNALISTICI *ONLINE* COME OCCASIONE PER INDIVIDUARE UN PUNTO DI EQUILIBRIO TRA DIRITTO ALL'OBLIO, ESIGENZE DI CANCELLAZIONE E TUTELA DELL'IDENTITÀ VIRTUALE

A conclusione di questa digressione, tanto densa quanto, appunto, necessariamente breve, vi è l'opportunità di notare come, nel caso di informazioni diffuse su Internet da un soggetto diverso dall'interessato sul presupposto di un interesse pubblico alla conoscenza di tali notizie, l'attenzione si sposti sempre di più sul piano della tutela dell'identità personale[155], e non più della riservatezza, poiché l'informazione originaria — ed è forse questo l'elemento principale che distingue le fattispecie in esame — è comunque intangibile ove ricorrano i requisiti che determinano la prevalenza, nel bilanciamento tra diritti, della libertà alla manifestazione del pensiero.

Sulla scorta di questa riflessione è inevitabile citare una recente sentenza della Corte di cassazione[156] la quale, prendendo atto della inadeguatezza della concezione classica del diritto all'oblio ove applicato alla realtà informatica, individua a favore dell'interessato i cui dati personali sono stati divulgati in rete (e che dunque rimangono pubblicamente accessibili, anche a distanza di tempo, con pregiudizio del diritto all'oblio) una forma di tutela alternativa alla cancellazione[157]: il diritto alla contestualizzazione dell'informazione.

Il motivo che ne giustifica il sintetico richiamo[158] in questa sede sta appunto nel collegamento della pronuncia con il mondo di Internet e nello spunto che può trarsi dallo sforzo della Suprema Corte di elaborare una possibile risposta ad un questione complessa come quella relativa alla fisionomia del diritto all'oblio in relazione ad informazioni oggetto di attività giornalistica e dunque, in definitiva, al bilanciamento tra diritti; tuttavia, il principio ivi enunciato, sebbene suscettibile di adattamento anche in tema di *cloud computing*, presenta limiti intrinseci che ne determinano l'applicazione a casi circoscritti e ne

---

154 *Ibidem*, p. 163, nota 53.

155 Il diritto all'oblio si colloca coerentemente in una prospettiva di autodeterminazione informativa e diviene «il mezzo per ricostruire la dimensione sociale dell'individuo, evitando che la vita passata possa costituire un ostacolo per la vita presente»: M. MEZZANOTTE, *Il diritto all'oblio*, cit., 121. Parimenti si avverte l'esigenza che la normativa sui dati personali sia compresa mediante «una lettura più alta e più ampia, che abbia ad oggetto la tutela della persona» e non solo le informazioni che la riguardano: riflessione sviluppata in G. FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. inf.*, 2012, 3, p. 388, dove si afferma addirittura che «il diritto alla protezione dei dati personali e i diritti della personalità ad esso limitrofi […] sono tutti volti a tutelare un unico bene giuridico: l'identità», declinata secondo i sui molteplici aspetti.

156 Cass. civ., sez. III, 5 aprile 2012, n. 5525, in *Nuova giur. civ. comm.*, 2012, I, p. 836, con nota di A. MANTELERO, Right to be forgotten *ed archivi storici dei giornali. La Cassazione travisa il diritto all'oblio*; in *Corr. giur.*, 2012, 6, p. 764, con nota di A. DI MAJO, *Il tempo siamo noi*… .

157 Il carattere innovativo della pronuncia è rilevato, apprezzato e difeso soprattutto da G. FINOCCHIARO, *Identità personale su Internet*, cit., pp. 383 ss., 392.

158 Più ampia ricostruzione in L. FEROLA, *Dal diritto all'oblio al diritto alla memoria nel* Web, cit., 1018 ss.

ostacolano l'inclusione tra i rimedi maggiormente efficaci e coerenti rispetto alle sfide poste dalle più moderne tecnologie della società dell'informazione.

La richiesta dell'interessato di ottenere la cancellazione dei dati memorizzati in un archivio *online* di una testata giornalistica ovvero, in subordine, il trasferimento dei medesimi in un'area non indicizzabile dai motori di ricerca esterni, era fondata sulla reperibilità, tramite generiche ricerche su Internet, della sola notizia riguardante l'avvio di procedimenti giudiziari nei suoi confronti, la quale non riportava i successivi sviluppi positivi della vicenda, conclusasi con il proscioglimento dell'imputato.

Il ricorso era stato rigettato sia dal Garante per la protezione dei dati personali sia dal Tribunale di Milano, i quali avevano evidenziato il non trascurabile elemento per cui il diritto all'oblio non avrebbe potuto comunque essere esercitato poiché, a causa della persistente notorietà del soggetto coinvolto, permaneva un interesse pubblico alla conoscenza delle vicende pregresse relative alla sua storia personale.

Il bilanciamento tra diritti fondamentali propugnato dalla Cassazione nel ribaltare le pronunce di grado inferiore si articola essenzialmente in due passaggi logici.

Il primo di questi consiste nell'affermazione della necessità di garantire all'interessato, a tutela della sua identità sociale, del dato oggetto del trattamento e «dello stesso diritto del cittadino utente a ricevere una completa e corretta informazione», una piena ed organica contestualizzazione delle notizie relative alle vicende che lo coinvolgono[159]. Il presupposto implicito si presta ad una duplice lettura[160]. Da un lato, potrebbe argomentarsi che l'interesse pubblico non può, per definizione, essere tale se non rivolto ad informazioni aggiornate: via chiaramente fallace, come dimostra la liceità di un trattamento rivolto a finalità di ricerca storica, rispetto alle quali è comunque individuabile un preciso interesse, anche costituzionalmente protetto. D'altra parte, una diversa via interpretativa potrebbe risalire fino a concepire la necessità di integrare un ulteriore parametro la cui presenza deve essere garantita in sede di controllo giurisdizionale con riguardo all'esercizio del diritto di cronaca: questo sarebbe identificabile con il requisito di "verità", il quale allora ben si mostra in grado di assorbire, *a fortiori*, il criterio dell'aggiornamento e dell'attualità[161].

La corrispondenza delle informazioni divulgate a verità e dunque la completezza della notizia nel riportare i fatti che ne formano oggetto rappresentano con tutta evidenza elementi solitamente considerati nel valutare i presupposti di legittimità della pubblicazione di eventi inerenti alla sfera

[159] Questo costituirebbe il vero e proprio «*thema decidendum*» della pronuncia, *sub specie* di ricerca di un diritto soggettivo dell'interessato all'aggiornamento delle notizie *online* che lo riguardano: F. DI CIOMMO – R. PARDOLESI, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza!*, in *Danno e resp.*, 2012, 7, p. 703.

[160] Ciò, ovviamente, a meno di non voler ammettere l'aggiunta di un «quarto requisito» autonomo su cui valutare la legittimità della cronaca giornalistica: v. P. LAGHEZZA, *Il diritto all'oblio esiste (e si vede)*, loc. cit.

[161] Questa pare la strada adottata dalla Suprema Corte: quando tale criterio non viene applicato, infatti, «la notizia, originariamente *completa e vera*, diviene *non aggiornata*, risultando quindi *parziale e non esatta*, e pertanto sostanzialmente *non vera*» (corsivo nel testo).

personale di un soggetto: pertanto la posizione innovativa della Cassazione può essere apprezzata soltanto comprendendo la necessità di una peculiare applicazione del principio citato in ragione delle caratteristiche specifiche della situazione all'esame della Suprema Corte.

Il secondo passaggio logico, infatti, il più interessante in questa sede, implica effettivamente — come sostengono le voci critiche[162] — l'equiparazione della memorizzazione della notizia in un archivio in rete ad una continua reiterazione della stessa o, quantomeno, ad una nuova divulgazione: questa dovrebbe allora soddisfare le condizioni consuete richieste per una legittima pubblicazione, tra cui soprattutto l'esattezza, da intendersi appunto come aggiornamento e contestualizzazione.

La prospettiva adottata della Cassazione confligge per di più con l'idea che la raccolta delle informazioni *online* dovrebbe essere intesa come una semplice conservazione documentale, in cui i dati componenti l'archivio valgono proprio in quanto reperti di una realtà in continuo fluire necessariamente fotografata in più istantanee frammentarie, ciascuna in sé completa in quanto assolvente la funzione di memoria storica in riferimento ad un preciso evento: al contrario, i giudici di legittimità sostengono come sia necessario garantire il collegamento della notizia «ad altra informazioni successivamente pubblicate concernenti l'evoluzione della vicenda, che possano completare o finanche radicalmente mutare il quadro evincentesi dalla notizia originaria», in questo modo giustificando la prospettiva di una eventuale (altrimenti inammissibile) alterazione della integrità dell'archivio[163].

IX.1. LE MOLTE OMBRE DEL DIRITTO ALLA CONTESTUALIZZAZIONE

Questa opera di contestualizzazione in senso lato presenta, se riferita in particolare agli archivi in rete, alcuni profili di notevole criticità.

Innanzitutto, si evidenzia una commistione tra finalità storico-ricostruttiva e finalità storico-archivistica[164], quest'ultima predominante nelle ipotesi in esame: la finalità di conservazione delle informazioni risulta assolta, come detto, solo in assenza di ogni modifica che vada ad incidere sulla rappresentazione veritiera del passato che ne forma oggetto e che ne ha originariamente giustificato la divulgazione. Al contrario, come riconosce la Cassazione stessa, l'opera di aggiornamento ed integrazione dei fatti diventa momento necessario (e, per così dire, essenziale) in caso di successiva rievocazione nell'esercizio delle attività giornalistica ovvero di ricerca storica, il significato delle quali

162 Spicca A. MANTELERO, Right to be forgotten, cit., p. 847.
163 La Cassazione richiede, per realizzare in concreto il principio di diritto affermato, «la predisposizione di un sistema idoneo a segnalare (nel corpo o a margine) la sussistenza di un seguito e di uno sviluppo della notizia». È comunque inevitabile percepire l'indeterminatezza delle modalità di aggiornamento suggerite, le quali risultano lacunose rispetto ai numerosi problemi che potranno verificarsi nella pratica: pur nel *favor* generale alla sentenza, conviene G. FINOCCHIARO, *Identità personale su Internet*, cit. pp. 393-394.
164 A. MANTELERO, *Il diritto all'oblio dalla carta stampata ad Internet*, cit., p. 160.

risiede proprio in una ricostruzione degli eventi inevitabilmente realizzata, sebbene con diverse finalità e diversi metodi, con riferimento al più ampio contesto delle vicende successive.

In definitiva, il requisito dell'aggiornamento dei dati dovrebbe essere valutato non tanto in base alla completezza del dato in sé, quanto rispetto alla finalità del trattamento[165]: ne risulta appunto ingiustificata l'imposizione di un obbligo di contestualizzazione a carico del titolare dell'archivio che pure rivesta il ruolo di *controller* e che dunque sia obbligato al rispetto delle disposizioni in materia di tutela dei dati personali, tra cui, appunto, di quelle relative alla qualità dei dati stessi.

In aggiunta, nonostante la crucialità della differenza tra archivi cartacei e banche dati digitali in termini di rischio di irragionevole esposizione agli occhi del pubblico — a nulla rilevando in ambito informatico il difetto di una "nuova narrazione" avvenuta nei modi tradizionali ai fini della tutela del diritto all'oblio dell'interessato, dovendosi quest'ultima calibrare sull'eterna permanenza in rete dei dati — la strada dell'aggiornamento non tiene conto del fatto che in fattispecie come quella all'esame della Suprema Corte «non si tratta di mere notizie reperibili mediante un motore di ricerca, rispetto alle quali può avere senso una riflessione sulle possibili soluzioni volte a favorirne una contestualizzazione, né di informazioni di cui non sia nota la fonte»[166].

La forma dell'archivio, infatti, presenta una forma organizzativa e una struttura organica tali per cui le singole informazioni sono corredate di elementi che ne garantiscono una precisa collocazione temporale, ne attestano la provenienza e comunque ne sottintendono la parzialità, suggerendo a chi vi ha accesso di procedere alla raccolta di dati ulteriori ai fini di ottenere un quadro il più accurato possibile. Non vi è motivo per credere che queste caratteristiche non siano mantenute in caso di trasferimento dell'archivio in rete: l'esigenza di contestualizzazione dovrà essere consequenzialmente indirizzata nei confronti dei contenuti disseminati in pagine *web* non organizzate, queste sì paragonabili a «pagine isolate di libri custoditi in mille diverse biblioteche»[167].

Infine, anche a voler prescindere dal tema delle difficoltà (probabilmente infinite) inerenti alla corretta ricostruzione di una presunta "verità storica", comunque riproponibili in ogni situazione in cui venga in rilievo la «salvaguardia dell'attuale identità sociale del soggetto cui [la notizia] afferisce»[168], in prospettiva digitale non può essere escluso che l'attività di aggiornamento delle informazioni incontri ostacoli tecnici simili a quelli precedentemente evidenziati in relazione alla cancellazione[169]: ad esempio, infatti,

---

165 *Ibidem*, p. 161, nota 51.

166 Ancora A. MANTELERO, Right to be forgotten, cit., p. 846.

167 G. FINOCCHIARO, *La memoria della rete*, cit., p. 395: è proprio in relazione a queste pagine che si evidenziano i principali problemi della conservazione dei dati su Internet, quali l'incertezza della fonte, l'inattendibilità dei contenuti e, appunto, la perdita dei consueti riferimenti spazio-temporali, da cui dipende il c.d. appiattimento delle informazioni.

168 Così ancora Cass. 5525/2012, cit. Avverte saggiamente dell'alto rischio di «tentazioni pirandelliane» G. FINOCCHIARO, *La memoria della rete*, cit., p. 399, la quale a sua volta cita A. FALZEA, *Il diritto all'identità personale: motivi di perplessità*, in AA. VV., *La lesione dell'identità personale e il danno non patrimoniale*, Milano, 1985, p. 89.

169 Colgono nel segno le osservazioni di F. DI CIOMMO – R. PARDOLESI, *Dal diritto all'oblio*, cit., p. 704.

una complessa procedura di contestualizzazione di una notizia, magari realizzata a seguito di approfondite e costose ricerche, anche qualora consentisse di mantenere i dati in perfetta aderenza con le vicende attuali che li coinvolgono, non potrebbe impedire la presenza diffusa di riproduzioni virtuali della notizia originaria nella sua versione non aggiornata[170].

La medesima questione, peraltro, è destinata a riproporsi con riferimento alla società dell'informazione fin quando non sia chiarito anche solo un punto apparentemente trascurabile, ma in realtà cruciale per comprendere le forme concrete della tutela apprestata in favore dell'interessato, relativo alla possibilità di qualificare come archivio ogni tipo di memorizzazione delle notizie *online* (anche e soprattutto quelle realizzate mediante servizi *cloud*): ove la risposta fosse affermativa[171], come potrebbe in ipotesi avvenire sulla scorta di considerazioni di prevalente natura tecnica inerenti alle caratteristiche dei contenuti e alla struttura dei siti Internet, sorgerebbero non poche difficoltà pratiche al momento dell'imposizione di un obbligo di aggiornamento e di contestualizzazione delle informazioni presenti su ogni pagina *web* e su ogni *server* in capo ai gestori del sito sorgente, poiché tale compito sarebbe a ragione ritenuto sproporzionato e inattuabile da parte della maggioranza degli utenti della rete[172]. Sebbene questi ultimi, nell'attuale contesto di fluidità delle comunicazioni informatiche, entrino in contatto con dati personali su base quotidiana, il passo verso una piena responsabilizzazione e un'estensione degli obblighi gravanti sul *controller* chiederebbe una precisa presa di posizione legislativa e, comunque, una riflessione più cauta e ponderata.

SEZIONE V

X. ALCUNI PUNTI FERMI

La percezione che accompagna la chiusura di questo contributo non è dissimile da quella che lo ha accompagnato in ogni pagina: così come chi scrive, anche il lettore avrà avvertito, in coincidenza non solo della presentazione di una qualunque questione, ma anche della formulazione di un'ipotesi di soluzione, un sollevarsi ininterrotto di problemi e, al contempo, una sensazione di insoddisfazione,

170 Similmente, tra gli aspetti problematici segnalati nella *Relazione annuale 2012* (p. 156), il Garante riporta il caso in cui, anche a seguito di un provvedimento di de-indicizzazione delle notizie in un archivio online, queste, dopo breve tempo, erano tornate facilmente reperibili mediante i motori di ricerca.

171 Sembra di leggere tracce in tal senso in F. DI CIOMMO – R. PARDOLESI, *Dal diritto all'oblio*, cit., pp. 713-714, ove si propende per l'immagine di Interne come «mare di archivi».

172 Ancora F. DI CIOMMO – R. PARDOLESI, *Dal diritto all'oblio*, cit., p. 705: si verificherebbe un fatale *chilling effect* sulle miriadi di piccoli e medi *provider* che «inseriscono contenuti quando vogliono, li aggiornano se e quando ne hanno la possibilità, assumendo spesso come principale obiettivo solo quello di immettere *online* dati ritenuti di interesse degli utenti» (basti pensare al gestore di un semplice — e comunissimo — *blog*).

tanto per i numerosi interrogativi che rimangono aperti, quanto per la difficoltà intrinseca di afferrarne l'essenza più profonda e la corretta impostazione.

Al di là degli ineliminabili difetti propri di ogni arte ermeneutica e "giurisprudenziale", le ragioni di un simile disorientamento dovrebbero essere ricercate nella specificità del substrato materiale cui si appunta la presente indagine: per questo motivo si è premesso alla trattazione un rapido tentativo di annotazione delle coordinate essenziali con le quali dovrebbe confrontarsi tanto le soluzioni normative quanto le applicazioni a singoli casi concreti.

Il loro valore sta proprio nella funzione di offrire un parametro di valutazione dell'effettività della tutela astrattamente offerta: la selezione degli interessi rilevanti ben può essere realizzata in una dimensione distinta, ma l'operatività dei meccanismi così elaborati dovrà appunto essere misurata su esigenze pratiche che trovano la propria radice nella tecnica e, ancor più, nella tecnologia.

Il carattere multiforme del *cloud computing*, emblematico del caleidoscopio delle possibili letture giuridiche del fenomeno Internet, restituisce all'interprete una visione spesso increspata dalle innumerevoli trame che si diramano in direzione di temi affini, concettualmente confinanti ma di cui è arduo stabilire la pregiudizialità o la consequenzialità rispetto all'analisi in corso.

Il reticolato diviene ancora più inestricabile quando vi si sovrappone l'ulteriore filtro di una figura amorfa come il "diritto all'oblio": sebbene non fosse questa la sede più idonea per condurre studi definitori o di inquadramento sistematico, quanto ancora sia sfuggente la fisionomia di tale diritto nonostante un certo sforzo in tal senso è dimostrato dalla prudenza grafica con la quale si è spesso tentati di menzionarlo.

Alla luce di tutto ciò, conviene forse ripercorrere in breve le tappe di questo studio e mettere a fuoco alcuni punti fermi, non senza il presentimento che anch'essi potranno al più servire come spunti per ulteriori riflessioni.

La diffusione dell'impiego di tecnologia *cloud* comporta di necessità un accentuarsi del rischio della perdita di controllo sui dati, evenienza in un primo momento trascurata ma rivalutata nella sua gravità al momento in cui, parallelamente a quella della memoria e della accessibilità rapida e diffusa delle informazioni in rete, si affermi l'esigenza della cancellazione delle medesime, in quanto ritenute lesive della riservatezza ovvero tali da compromettere in futuro la reputazione, con conseguenze facilmente (o difficilmente) immaginabili. In un'ottica di apertura all'intervento legislativo in materia, premessa la insufficienza della tutela all'interessato concessa sotto il regime attualmente vigente rispetto alle insidie della tecnologia *cloud*, l'attenzione è stata indirizzata alla innovazione costituita dalla proposta di regolamento elaborata a livello di Unione Europea.

La previsione esplicita di un «diritto all'oblio e alla cancellazione» ad opera dell'art. 17, tuttavia, ad una lettura più approfondita del testo che tenga pure in considerazione lo scenario dei meccanismi di tutela offerti dalla direttiva, non mostra particolari elementi di novità: molte ipotesi in cui è riconosciuto il rimedio della eliminazione dei dati dal sistema del responsabile del trattamento possono essere fatte coincidere con i casi ricavabili e ricavati in via ermeneutica dalla disciplina attuale, che il legislatore europeo pare avere soltanto esplicitato e puntualizzato[173].

A riprova di ciò, un mutamento significativo dal punto di vista sostanziale non si registra neppure a seguito del tentativo di sondare le prospettive di applicabilità dell'art. 17 ai servizi di *cloud computing*: per questi sussistono problemi legati sia alle caratteristiche comuni alle tecnologie informatiche sia alle specificità che, soprattutto in relazione al principio di finalità del trattamento, ne contraddistinguono l'impiego sul piano dei rischi per la *privacy*. Peraltro, si è tentato di dimostrare come il potenziale intrinseco alla presunta rivoluzione legislativa risieda in buona parte, in tema di diritto alla cancellazione, nella previsione del par. 2 del medesimo articolo, laddove emerge con più nitidezza la presa coscienza della necessità di plasmare la disciplina a tutela dei dati personali sulla scorta delle strette relazioni virtuali che intercorrono tra soggetti non determinabili *a priori* ma che possono comunque entrare in contatto a vario titolo con informazioni dell'interessato: sul punto si rivelerà poi imprescindibile l'intervento chiarificatore della Corte di giustizia, la quale potrà sciogliere molti dei nodi sulla questione qualificando il ruolo dei terzi ed individuando, si presume con metodo di interpretazione sistematica, la portata dei rimedi che potranno coinvolgerli in caso di inottemperanza della richiesta loro rivolta.

Tuttavia, la tesi sostenuta in questo contributo discende dall'enucleazione di una questione pregiudiziale ad una efficace applicazione dell'art. 17 al *cloud computing*, costituita dalla necessità di individuare nella realtà i soggetti corrispondenti alle categorie astratte di *controller* e *processor*: per ovvia delimitazione materiale del campo di analisi non si è potuto che accennare al tema, ma nel corso della trattazione si è evidenziato come esso risulti cruciale per comprendere a pieno il grado di tutela offerto all'interessato e per assicurarne il rispetto nel modo più coerente al carattere fluido e aformalistico della società dell'informazione.

Sempre nell'ottica di una valutazione in concreto della futura implementazione di un diritto alla cancellazione, lo si è visto, risulta inevitabile confrontarsi con numerosi ostacoli, di tipo sia tecnico sia giuridico, alcuni dei possono ricavarsi da preesistenti indici rintracciabili in pronunce significative dei giudici di Lussemburgo, la cui opera ermeneutica in campo di diritto di Internet si è mostrata tanto attenta ai diritti della persona quanto lucidamente consapevole delle altre istanze, di ordine economico e sociale, emergenti a causa dell'arricchimento esponenziale delle variabili e degli interessi in gioco, in

173 Cfr. A. MANTELERO, *U.S. Concern*, cit., pp. 734-735: «*Article 17 is more analytical in defining the right […] but the various cases [in which the right can be invoked] are still within the two main hypotheses already defined, albeit more rigidly, by the Directive 95/46/EC in force*».

corrispondenza con i nuovi sviluppi tecnologici. Tuttavia, ancora una volta, la compatibilità dei principi così elaborati rispetto al *cloud computing*, nonché la loro idoneità a perseguire la propria funzione in un ambito al momento pressoché inesplorato dagli operatori, dipendono dall'attribuzione dei doveri e delle responsabilità collegati alle figure previste dalla disciplina in materia di *privacy*.

A questo complesso bilanciamento, la cui uniformità potrà essere agevolata ma non garantita dall'adozione del regolamento, stante comunque la presenza di uno spazio di manovra per i singoli Stati membri in considerazione del coinvolgimento (anche) di diritti fondamentali, non potrà sottrarsi neppure il diritto alla cancellazione riconosciuto all'art. 17: in particolare, una incognita su cui non è stato possibile soffermarsi, ma che meriterebbe attenzione in ragione delle sue molteplici implicazioni, è quella relativa alla libertà di espressione e d'informazione, che voci preoccupate ritengono a rischio di essere ingiustificatamente sacrificata nel momento in cui fosse concessa la facoltà per l'interessato di ottenere l'eliminazione dei propri dati personali in base ad una scelta di mera opportunità e, dunque, come tale, puramente arbitraria.

XI. QUESTIONI CONCLUSIVE; IN PARTICOLARE, IL NODO DELLO *USER-GENERATED CONTENT*

Chiarite le grandi linee dell'itinerario logico che si è tentato di percorrere — e dal quale è stato talvolta inevitabile allontanarsi di qualche passo, tentati da altri sentieri non sempre secondari — conviene spiegare meglio il valore del riferimento finale alla costruzione concettuale italiana del "diritto all'oblio", dal quale sarà possibile trarre spunto per una riflessione finale.

Il primo problema da tenere in considerazione è di natura nominalistica: come segnalato, il regolamento innova anche sul piano del recepimento a livello di legislazione dell'Unione della formula «diritto all'oblio», affiancata con prudenza, nella rubrica dell'articolo, dall'aggiunta «e alla cancellazione»[174]. In realtà, per le caratteristiche che si sono evidenziate, l'art. 17 pare applicabile principalmente con riferimento alle fattispecie in cui ricorra un trattamento illecito dei dati o siano venute meno le condizioni legittimanti il trattamento e alle quali si riconosce appunto il rimedio della eliminazione dei dati dal sistema informatico del *controller*: il nucleo essenziale della disposizione risiede, infatti, nella predisposizione di una forma di salvaguardia per l'interessato tale da consentire, da un lato, la rimozione

[174] Questa endiadi mal riuscita genera effettivamente «una confusione terminologica e concettuale nella misura in cui viene utilizzata la definizione "*right to be forgotten*" con riferimento alle ipotesi di mera cancellazione»: M. SIANO, *Il diritto all'oblio in Europa e il recente caso spagnolo*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, cit., p. 131.

dei dati esposti, dall'altro la sottrazione degli stessi al rischio di trattamenti successivi, senza dunque fratture concettuali nette con la direttiva[175].

Il motivo per il quale sembra di poter intendere la dizione «diritto all'oblio» come forma enfatica di un più realistico (e reale) diritto alla cancellazione[176], il solo ad essere riconosciuto nella pratica dall'art. 17, risiede nel disegno complessivo della disciplina europea: se, infatti, si ricordano anche le riflessioni svolte in merito al ruolo del consenso nell'architettura del regolamento, si coglie come l'obiettivo del sistema sia proprio la tutela dei dati personali nelle inevitabili relazioni con l'esterno in cui essi sono attratti e il conferimento all'interessato di appositi strumenti di controllo delle varie vicende dei dati stessi. Inoltre, a ben guardare, il bene giuridico protetto, seppure in via mediata, dal diritto alla cancellazione è il diritto alla riservatezza, inteso come pretesa a non vedere invasa la sfera della propria vita personale nei suoi aspetti più intimi: l'eliminazione dell'informazione è intesa come rimozione da dove questa non dovrebbe stare, poiché, sebbene in origine privata, non lo è rimasta ed è illegittimamente conoscibile da altri, i quali potrebbero persino procedere ad ulteriori trattamenti con il rischio di ancor più ampia diffusione.

In questa ottica il diritto alla cancellazione, per quanto parallelo, rimane ben distinto dal "diritto all'oblio" vivente nell'esperienza applicativa italiana[177], che si è ritenuto opportuno riportare nel suo sviluppo più recente e più controverso per meglio sottolineare le differenze rispetto al presunto omologo europeo.

La prospettiva in cui si inserisce la ricostruzione giurisprudenziale nazionale, come si evince dalla stessa definizione della fisionomia del diritto in questione, implica un'attenzione specifica per il danno che la divulgazione dei dati potrebbe cagionare all'identità personale dell'interessato.

Questa visuale particolare, per quanto non esaurisca la gamma di profili problematici connessi alla tutela della persona rispetto ai suoi dati personali, si rivela assai utile in quanto racchiude una potenziale risposta ad una questione di grande attualità: in tal senso, peraltro, al di là delle critiche qui riportate, è apprezzabile la soluzione adottata dalla Cassazione nella sentenza citata.

---

175 Sulla cui idoneità a garantire un diritto all'oblio di portata generale si è tuttavia espresso negativamente l'avvocato generale nelle conclusioni alla causa C-131/12.

176 Come spesso accade, i problemi nominalistici trovano soluzione in una prospettiva sostanziale: indipendentemente dall'etichetta verbale che vi si appone, occorre chiarire, infatti, alcuni aspetti di fondo mediante un approccio descrittivo al diritto in questione. Questa strada è segnata dalle domande: «Vi è (o vi dovrebbe essere) un diritto di controllo assoluto, sciolto da ogni vincolo, del soggetto cui le informazioni si riferiscono? O questi deve dimostrare che vi è lesione della sua identità personale? O che la legge sulla protezione dei dati non è stata rispettata? È necessario un bilanciamento con altri diritti?» (G. FINOCCHIARO, *La memoria della rete*, cit., p. 398). Anche ad interrogativi di tal genere si è tentato di dare risposta o, quantomeno, di pensare con spirito critico: in ciò risiede l'anima essenziale di questo contributo.

177 Ad esempio, in termini rigorosi e per questo efficaci, il diritto all'oblio è incompatibile con le ipotesi di cancellazione dei dati fondate sulla revoca del consenso, poiché nella genetica del diritto stesso non si pone neppure un problema relativo al consenso, stante la sussistenza di tutt'altra forma di legittimazione del trattamento: v. A. MANTELERO, *Il diritto all'oblio dalla carta stampata ad Internet*, cit., p. 166, nota 59.

Emerge infatti la necessità di predisporre meccanismi di salvaguardia che non prescindano dalle manifestazioni poliedriche della identità del singolo, astrattamente negando un fenomeno sociale e persino culturale di notevoli dimensioni, quale la proteiforme e frammentata rappresentazione di sé, ma sappiano offrire una risposta adeguata che tenga conto della necessità di mantenere una connotazione relazionale multiforme e del fatto che ciò avviene sempre più spesso, in modo diretto o indiretto, attraverso il conferimento e la diffusione di dati personali in rete.

Per parafrasare il titolo di un'opera divenuta metafora ormai abusata, sarebbe utopistico voler ridurre centomila volti addirittura ad uno o addirittura a nessuno, con la conseguenza di un'obliterazione alle volte controproducente per lo stesso richiedente, mentre più sensato risulterebbe — si specifica: sempre nell'ottica di una dimensione in cui la pluralità dei rapporti, anche se virtuali, tra individui è un aspetto percepito come fondamentale — non sacrificare l'intera propria esistenza digitale, quanto riaffermare la stessa, con gli strumenti appropriati, in termini aderenti alla verità, così da garantire che centomila volti appaiano, non deformati, ciascuno entro i propri lineamenti.

Ne consegue che l'avversione di fondo verso una cancellazione totale dei dati, solitamente giustificata, a prescindere dalla fattibilità dell'operazione sul piano tecnico, sulla base dell'interesse pubblico che ha legittimato l'originaria divulgazione della notizia, potrebbe rivelarsi condivisibile e dunque riproponibile, sebbene in relazione ad altri presupposti, anche con riguardo a fattispecie di diverso tipo.

D'altra parte, non si è mancato di far notare come sia possibile che lo stesso interessato prediliga, piuttosto che far cadere un velo di oblio sulla propria figura, la rimozione selettiva di alcune informazioni sconvenienti, con l'obiettivo non tanto di tornare nell'anonimato, quanto di presentare alla platea di destinatari delle sue comunicazioni, alle quali non desidera abdicare, una migliore immagine di sé.

Sotto questo aspetto, si potrebbe suggerire, il riconoscimento di un diritto alla cancellazione generalizzato rappresenta una regressione alla concezione di *privacy* intesa come *right to be left alone*, dunque incentrata su una rigida condizione di riservatezza: ciò contrasta, almeno in termini empirici, con la tendenza, registrabile soprattutto su Internet, ad esporre e persino a sovra-esporre la propria sfera privata mediante il conferimento incontrollato di informazioni personali, in cambio di prestazioni gratuite ovvero, in ipotesi altrettanto numerose, al fine di usufruire di servizi diretti proprio all'implementazione delle attività sociali e relazionali. La realtà dei *social network* e, più in generale, del *cloud computing* offre appunto un esempio emblematico della necessità di propendere per una graduazione del "diritto all'oblio" coerente con il concetto di tutela dell'identità dinamica in ambito informatico[178].

[178] Non casuale il riferimento a (e in) F. DI CIOMMO – R. PARDOLESI, *Dal diritto*, cit.

Il ragionamento è avvalorato indubbiamente dall'esigenza di non ostacolare lo sviluppo armonioso del servizio tecnologico di *cloud* attraverso l'imposizione di una disciplina irragionevole perché, prima ancora che eccessivamente rigorosa, tecnicamente ed economicamente (oltre che socialmente) inattuabile, e dunque tale da scoraggiare sul nascere gli investimenti su una tecnologia innovativa di riconosciuto valore per il mondo delle imprese a livello globale e, per quanto interessa in questa sede, soprattutto in una prospettiva di consolidamento del mercato unico europeo[179]. La stessa considerazione dovrebbe comunque valere per eventuali obblighi di contestualizzazione e di continuo aggiornamento dell'informazione tali da gravare in modo irragionevole sul prestatore del servizio o sul responsabile del trattamento.

Alla luce di tutte le riflessioni precedenti, la conclusione che si vuole proporre consiste in un duplice interrogativo, per il quale questo lavoro può fornire lo spunto, ma non la soluzione. Le due domande sono tra di loro strettamente collegate: innanzitutto converrebbe chiedersi se l'intera questione affrontata possa essere riformulata mediante un approccio sistematico fondato su una più accurata distinzione delle fattispecie rilevanti in base alle circostanze oggettive e soggettive di conferimento dei dati personali, così da poter adeguatamente valutare l'ammissibilità, prima ancora che la portata, del diritto all'oblio e, allo stesso tempo, del rimedio della cancellazione.

Una volta adottata una simile prospettiva si schiude il quesito forse più affascinante e che attraversa in modo trasversale e sotterraneo gran parte dei temi trattati, con particolare attinenza al fenomeno del *cloud computing*: il "diritto all'oblio", quando non riguardi informazioni diffuse da mezzi di comunicazione di massa nel rispetto dei principi di verità, pertinenza e continenza, bensì dati conferiti volontariamente dall'interessato e da questi resi accessibili al pubblico, nel contesto della fruizione di un servizio in rete, deve essere esercitato limitatamente ai casi di lesione dell'identità oppure può considerarsi suscettibile di applicazione ad altre fattispecie? È concepibile una versione spuria, più vicina ad un "diritto alla cancellazione" di portata generale, come quello oggi paventato (ma inesistente)?

La questione si riconduce alla necessità di chiarire la portata e l'applicazione delle regole rilevanti a livello europeo con riferimento alle possibili combinazioni dei rapporti che nella realtà dei fatti intercorrono tra interessato, responsabile del trattamento e titolare del trattamento; di riflesso, e in misura forse preponderante, lo statuto dello *user–generated content*[180] nell'ambito della nozione di dato

[179] *Rectius*, «*the Digital Single Market*»: cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Unleashing the Potential of Cloud Computing in Europe*, COM(2012) 529 final, Bruxelles, 27.9.2012; rivoluzionario il cambiamento prefigurato in European Commission's *Proposal for a Regulation of the European Parliament and of the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent*, COM(2013) 627 final, Bruxelles, 11.9.2013.

[180] Come spunto, si osservi che il "diritto all'oblio" emergente dalla proposta di regolamento «*seems to fail to distinguish between two kinds of online user-generated material: «1) material about the data subject which the data subject herself has put on the provider's platform; 2) material about the data subject that other users have put on the provider's platform*»: così magistralmente G. SARTOR, *Providers' liabilities in the new EU Data Protection*

personale e della protezione dei diritti alla riservatezza e all'identità personale, i rapporti con le nuove tecnologie informatiche e con il fenomeno della condivisione, sempre più diffuso e caratteristico dei servizi in rete, a cui si ricollega il problema dell'attrito con il principio di finalità, rappresentano temi di frontiera[181] accomunati dall'esigenza e dal compito per l'interprete di elaborare una risposta innovativa e al tempo stesso efficace sul piano della tutela della persona, sia nei suoi aspetti materiali che immateriali, nella consapevolezza dell'attualità di una prospettiva rimediale di tipo non solo risarcitorio.

Regulation: a threat to Internet freedoms?, EUI Working Paper, Law, No. 2012/24, p. 10; altri indizi in J. ROSEN, *The right to be forgotten*, cit.; O. POLLICINO – M. BASSINI, *Diritto all'oblio*, cit., p. 224; A. MANTELERO, *U.S. Concern*, cit., p. 740; L. FEROLA, *Dal diritto all'oblio*, cit., p. 1028; F. DI CIOMMO – R. PARDOLESI, *Dal diritto all'oblio*, cit., pp. 715-716.

[181] Il concetto può anche essere sintetizzato con un'ulteriore domanda: può oggi ritenersi ancora valida la riflessione proposta in tempi non recenti da Cass. civ., sez. I, 22 dicembre 1956, n. 4487, in *Foro it.*, 1957, I, cc. 4 ss., secondo cui «chi non ha saputo o voluto tener celati i fatti della propria vita privata, non può pretendere che il segreto sia mantenuto dalla discrezione altrui»?