ITALIAN ACADEMY OF THE INTERNET CODE

POSITION PAPER

GOVERNANCE DI INTERNET ED EFFICIENZA DELLE REGOLE: VERSO IL NUOVO REGOLAMENTO EUROPEO SULLA PRIVACY

Sommario: 1. Governance di Internet ed efficienza delle regole nell'ottica della concorrenza. – 2. Big Data Scenario. – 3. L'importanza dell'approvazione del regolamento europeo sulla privacy: la necessità di paradigmi comuni nell'economia globalizzata. – 4. One Stop Shop ed efficienza dell'azione di vigilanza. – 5. Il consenso al trattamento secondo l'approccio basato sul rischio. – 6. Il diritto all'oblio.

1. *Governance* di Internet ed efficienza delle regole nell'ottica della concorrenza.

La Commissione europea ha evidenziato in più occasioni[1] come lo sviluppo dell'economia digitale nell'Unione Europea negli ultimi anni è stato complessivamente meno rapido ed efficiente rispetto all'evoluzione avuta negli Stati Uniti, con il consequenziale e naturale riverbero sulle attuali capacità industriali degli operatori europei. Anche i finanziamenti europei, nell'ambito dell'innovazione e della ricerca in materia di tecnologie digitali, si sono rivelati al di sotto della massa critica e le attività a tutt'oggi presenti in questo campo si dimostrano scarsamente coordinate tra loro.

Questa situazione è riscontrabile in generale con riferimento a tutti i tipi di attività nel campo dell'ICT pur palesandosi con massima evidenza nei più innovativi servizi coniati. Ci si riferisce, in particolare, ai servizi di *cloud computing*, di *crowdsourcing* e ai *big data*.

Elemento essenziale che connota tali servizi è il naturale ambito di erogazione degli stessi che prescinde dal territorio in cui è stabilito il *provider* per assumere dimensioni globali sia per ragioni tecniche che per ragioni economiche.

[1] Cfr. *General approach to modernize the European data protection regime Position of the Industry Coalition for Data Protection*, Overview of the position of the Industry Coalition on Data Protection (ICDP) – November 2014

Le prime afferiscono alla possibilità di erogare i servizi in tempo reale da qualsiasi punto della rete, mentre le seconde attengono agli ingenti investimenti richiesti ai *provider* per la creazione delle infrastrutture per l'erogazione dei servizi e dunque alla necessità di avere la possibilità di rientrare di detti investimenti attraverso efficienti economie di scala.

In questo contesto si palesa come la possibilità di operare in mercati transnazionali richiede la necessaria definizione di regole normative comuni applicabili a tutti gli utenti, non essendo ipotizzabile che i *provider* sopportino i costi per approntare diversi condizioni a seconda della nazionalità dell'utente.

L'esigenza di definizione di un quadro normativo quanto più ampio possibile viene percepita dai legislatori non tanto con riferimento alle regole civilistiche che sovraintendono ai rapporti contrattuali tra utenti e *provider*, ma piuttosto alla regolamentazione dei diritti della persona la cui tutela viene ritenuta non attribuibile unicamente alla forza contrattuale delle parti, specie per quanto attiene alla tutela della privacy degli utenti.

2. Privacy e Big Data Scenario

Uno dei servizi dell'ICT che palesa maggiori prospettive di crescita è indubbiamente quello dei *big data*, termine con il quale, come è noto, si fa riferimento all'elaborazione di grandi quantità di dati di tipo diverso, raccolti da fonti eterogenee per il successivo collezionamento in *dataset* di rilevanti dimensioni.

Le potenzialità di tali *collection*, sotto il profilo della creazione e gestione del valore, sono di dimensioni inimmaginabili. Nel 2012 questa frontiera ha stimolato una spesa mondiale di ventotto miliardi di euro, che ha raggiunto quota trentaquattro miliardi l'anno successivo. Le stime più recenti valutano che il mercato europeo dei *big data* sia pari al 30% del mercato mondiale dei dati e che in esso si potranno avere, entro il 2020, fino a centomila nuovi posti di lavoro, oltre a benefici indiretti quali la riduzione del 10% di consumi energetici, una migliore assistenza sanitaria e macchinari industriali più efficienti. Alla luce di questi dati, la Commissione europea, con l'ausilio di alcuni fornitori di ICT, si è impegnata ad investire complessivamente due miliardi e mezzo di euro per partenariati pubblico-privati, mentre cinquecento milioni di euro sono stati già previsti nei fondi del programma Horizon 2020, per cinque anni (2015-2020) [2].

Gli importi degli investimenti, prevedibili e previsti, dimostrano un'innovazione in corso e la volontà di avviare una nuova rivoluzione industriale basata sulla possibilità di accelerare le attività umane ed i processi produttivi attraverso le nuove modalità di impiego dei dati, così favorendo la comparsa di nuovi prodotti e servizi commerciali.

Nella recente Comunicazione del 2 luglio 2014 la Commissione europea ha evidenziato come lo stato di avanzamento dell'economia digitale nell'Unione Europea sia più lento rispetto agli Stati Uniti, nonostante le nuove opportunità economiche che

[2] Comunicazione Commissione Europea 13 ottobre 2014

discendono dai processi di digitalizzazione delle aziende e delle pubbliche amministrazioni, in ragione della necessaria modernizzazione degli apparati burocratici, dell'economizzazione dei servizi *tout court* e dell'ottimizzazione dei processi di archiviazione, trasferimento, elaborazione e analisi dei dati[3].

Si pensi che, sempre stando ai dati della Commissione europea, il 5% del PIL europeo viene generato dal settore dell'*Information Communication Technology* (ICT) applicata proprio ai dati sui servizi pubblici all'interno del PSI, e in attuazione dell'omologa direttiva i vari legislatori nazionali hanno adottato un'apposita regolamentazione volta a disciplinare specificamente gli aspetti economici[4].

Una delle più rilevanti ragioni della sproporzione tra gli investimenti tra operatori europei e statunitensi, a fronte degli appena richiamati incentivi legislativi allo sviluppo del mercato dei *big data*, pare essere rinvenibile, dunque, nell'attuale complessità del quadro giuridico e alla difficoltà di accedere a grandi *dataset* e infrastrutture abilitanti. Tali elementi si traducono, infatti, in barriere che ostacolano l'ingresso sul mercato delle PMI che dovrebbe essere, invece, le prime generatrici di innovazione[5].

La struttura tecnica delle infrastrutture *big data* comporta modalità di trattamento dei dati ivi contenuti che per necessità prevede il continuo scambio tra diversi soggetti, *rectius* titolari del trattamento dati, posti in diversi continenti, caratteristiche che palesa la difficoltà dal lato degli operatori ad affrontare diverse normative in materia di trattamento dei dati.

Ciò è tanto vero che, all'interno del pacchetto di riforme predisposto in questi ultimi anni dalla Commissione europea in materia di trattamento dei dati, è stata attribuita una posizione preminente ai *big data*. In particolare l'obiettivo che la Commissione intende perseguire è la definizione di un contesto normativo solido, in grado di preservare la fiducia degli utenti nell'ambiente digitale, maturando al contempo uno spazio sicuro dove beni e servizi possano svilupparsi ampiamente.

Invero lo scenario che si presenta non coinvolge solamente la materia della riservatezza, ma anche l'ambito la tutela dei consumatori (nella misura in cui le tecniche di *marketing* fanno ampio uso della tecnologia dei *big data*) e quella della tutela della concorrenza (avuto riguardo all'elevatissimo potenziale economico di cui i *big data* sono rivestiti)[6].

3. L'importanza dell'approvazione del regolamento europeo sulla privacy: la necessità di paradigmi comuni nell'economia globalizzata

[3] M.C. De Vivo, A. Polzonetti, P. Tapanelli, *Open Data, Business Intelligence e Governance nella Pubblica Amministrazione*, in *Informatica e diritto*, n. 2/2011

[4] Si veda i cc.dd. "Decreto trasparenza", il "Decreto sviluppo" e il "Decreto crescita 2.0", nonché il D. Lgs. n. 36/2006.

[5] V. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Verso una florida economia basata sui dati,* 2 luglio 2014.

[6] V. COM(2014)442

L'auspicio di una regolamentazione dell'Internet efficiente discende dalla necessità di una maggiore considerazione dei diritti della persona nel nuovo scenario tecnologico, ossia dei c.d. diritti di quarta generazione.

Come noto, l'approccio europeo è stato assai differente rispetto a quello statunitense. Infatti, anche se il Congresso statunitense ha tentato di elaborare una disciplina omogenea a tutti gli Stati membri[7], negli Stati Uniti la regolamentazione della privacy è andata crescendo all'interno delle Corti di Giustizia, le quali hanno optato per un metodo *laissez-faire* sulla cui base i settori non regolamentati sono stati obbligati ad adottare un'autoregolamentazione specifica dei dati privati. Viceversa in Europa la modalità con cui si è tentavo di tutelare la privacy è stata quella di emanare un'apposita direttiva: la dir. 95/46/CE parte dal presupposto che la tutela della privacy è un diritto fondamentale dell'individuo e, nonostante consenta la libera circolazione delle informazioni tra i vari Stati membri, impone il rispetto di una dettagliata disciplina delle modalità di trattamento dei dati personali[8].

Proprio la collocazione europea della tutela della privacy nella categoria dei diritti fondamentali dell'uomo consente di rispondere all'interrogativo di chi, negli Stati Uniti, si è domandato quale fosse la necessità di una direttiva sul tema, laddove, viceversa, i dati personali rappresentano un bene da sfruttare e che assicurano un ritorno economico.

L'analisi dell'impatto della normativa sul trattamento dei dati ha dimostrato come il rallentamento dello sviluppo dell'economia digitale non discenda unicamente dalla previsione di una dettagliata normativa in materia ma, piuttosto, dalle modalità non uniformi con cui la direttiva è stata recepita nei singoli Stati membri.

A distanza di quindici anni dall'emanazione della prima direttiva sul tema, tenuto conto del mancato raggiungimento dell'obiettivo di definizione di un quadro normativo uniforme sul territorio europeo e considerato il mutato scenario tecnologico, l'Unione Europea ha cominciato a pensare ad un regolamento che consentisse l'armonizzazione della disciplina in materia di *privacy* negli ordinamenti dei vari Stati membri.

L'opportunità dell'armonizzazione degli ordinamenti giuridici dei vari Stati membri si rende necessaria con riguardo alla materia della privacy per tutta una serie di fattori.

In primo luogo per il fatto che, sulla scorta della proposta di regolamento europeo sulle firme elettroniche del 4 giugno 2012, si è inteso eliminare il costo derivante dalle diverse modalità di applicazione della direttiva, così come si intende consentire ai titolari delle operazioni di trattamento dei dati un risparmio sull'adeguamento alle varie legislazioni nazionali.

Lo scorso 21 ottobre 2013 la Commissione Libertà civili e giustizia del Parlamento UE (LIBE) ha ricevuto in tal senso formale mandato per avviare i negoziati con il Consiglio al fine di raggiungere un accordo comune sul Regolamento *Data Protection*[9].

---

[7] V. USA Patriot Act del 2001 che ha incrementato i poteri del Governo federale con riguardo ai procedimenti di accesso ai dati detenuti dalle imprese.

[8] E. R. ALO, *EU privacy protection: a step towards global privacy,* Michigan State International Law Review, p. 1096 ss.

[9] Cfr. *General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)*.

Sebbene l'obiettivo fosse quello di emanare il regolamento entro la fine del 2014, l'adozione del regolamento è ora atteso per il 2015.

Invero, pur non discostandosi molto dai contenuti della precedente disciplina, la proposta di regolamento si sofferma su alcuni punti focali che consentiranno la definizione di un quadro normativo unitario in grado di favorire lo sviluppo dei nuovi servizi dell'ICT. Tra gli elementi più rilevanti della proposta di regolamento è opportuno segnalare la nuova modalità di prestazione del consenso al trattamento dei dati personali connesso al calcolo del rischio, la profilazione dell'utenza e la disciplina del diritto all'oblio, c.d. *right to be forgotten*. In questo senso, la proposta di regolamento imporrà le condizioni previste al suo interno a tutti gli Stati che vorranno operare nel mercato europeo[10].

4. One Stop Shop ed efficienza dell'azione di vigilanza.

La Direttiva 95/46/EC non identifica meccanismi di coordinamento e/o cooperazione tra le Autorità garanti dei vari Stati membri, carenza che comporta per un'impresa che opera in più Stati membri l'obbligo di confrontarsi con più Autorità nazionali, che a loro volta sovraintendono all'attuazione di potenziali differenti disciplina di attuazione.

L'Art. 28(4) della Direttiva 1995 precisa che ogni soggetto interessato può segnalare comportamenti pregiudizievoli alla propria Autorità (locale), anche se l'Autorità competente e procedente sarà quella del luogo in cui ha sede la società che processa dati, indipendentemente dal fatto che gli effetti si producano altrove (Article 4(1) (a), (b) and (c) of Directive 95/46/EC).

Tale scelta legislativa risulta essere giustificata quando il trattamento si realizza e i suoi effetti si riflettono all'interno dei confini nazionali, all'interno cioè di un contesto locale.

Tuttavia, quando il trattamento non esaurisce i suoi effetti all'interno dei confini nazionali, quando cioè ci si confronta con comportamenti dall'impatto transfrontaliero il modello vacilla perché non è idoneo a garantire la certezza del diritto e le legittime aspettative degli interessati, nonché non appare adeguato a rispondere alle esigenze che derivano dalla globalizzazione dei mercati e dalla sfida dell'economia dell'informazione e della conoscenza.

In altri termini, il modello in essere presenta limiti giuridici in ordine all'incertezza giuridica, alla frammentazione delle procedure, alle disparità di trattamento e di protezione - anche in ragione di risorse non omogenee e priorità non allineate -, nonché riversa i costi economici di questa frammentazione sugli operatori che sono così

[10] Cfr. *General approach to modernize the European data protection regime Position of the Industry Coalition for Data Protection*, Overview of the position of the Industry Coalition on Data Protection (ICDP) – November 2014

disincentivati dalla prestazione di servizi transfrontalieri anche nell'ambito del territorio europeo.

Dalle criticità emerse risulta chiara l'opportunità di sostituire un modello di competenze distribuite con un modello accentrato condiviso, chiaro e prevedibile disegnando in maniera netta la linea di demarcazione tra trattamenti puramente locali e trattamenti di rilevanza transnazionale, ancorandola allo stabilimento e agli effetti in via cumulativa e traslare *progressivamente* il modello dello sportello unico, avvalendosi dell'esperienza maturata in altri settori del diritto comunitario laddove ha consentito di risolvere i conflitti di attribuzioni e competenze, accentrare la valutazione di comportamenti suscettibili di essere valutati da più Autorità, e ciò per realizzare la finalità della convergenza delle decisioni in presenza di specifici presupposti.

Il meccanismo del *one stop shop* è chiamato ad operare solo in presenza di condotte di rilevanza transnazionale, se ricorre un presupposto statico, legato alla pluralità di sedi dell'impresa, ovvero se ricorre una condizione dinamica, vale a dire se la condotta comporti attività e determini effetti che superano i confini nazionali. Opera cioè se ricorrono requisiti tali da qualificare il comportamento all'esame come transfrontaliero, idoneo cioè ad incidere in maniera sostanziale su soggetti residenti in più Stati membri.

È di tutta evidenza peraltro l'approdo ad un quadro normativo armonizzato non può prescindere dalla previsione che lo stesso *enforcement* del diritto fondamentale della protezione dei dati personali sia conforme ai principi di convergenza, coerenza e non contraddizione nelle prassi nazionali.

5. Il consenso al trattamento secondo l'approccio basato sul rischio.

Come anticipato uno dei punti focali del pacchetto di riforma è la c.d. *Data Protection Impact Assessment* (DPIA), una procedura di analisi dei rischi che mira a ponderare *ex ante* l'incidenza che una determinata soluzione tecnica avrà sulla tutela dei dati trattati. L'analisi viene effettuata caso per caso, in ragione delle specificità correlate alle modalità di gestione delle informazioni.

Questa procedura, già presente in alcuni Paesi, ha preso piede anche nell'ambito dell'Unione in relazione ai dispositivi di identificazione a radio frequenza, c.d. Rfid, al fine di stimolare i produttori a sviluppare tecnologie rispettose della normativa sulla *privacy*. Tale mezzo di carattere preventivo, infatti, dovrebbe essere teso a valutare se il trattamento dei dati svolto nell'ambito della prestazione di un servizio sarà effettuato in maniera conforme alle disposizioni in materia, in modo da adottare prontamente le modalità di protezione che risultino necessarie.

La DPIA si colloca, dunque, in una fase preliminare dello sviluppo del prodotto/servizio, quando il *design* di quest'ultimo non è delineato in maniera

definitiva, bensì è ancora in uno stadio progettuale. Uno dei vantaggi derivanti dall'adozione della DPIA consiste nella possibilità di ricorrervi non solo nella fase iniziale di progettazione, essendo uno strumento valutativo del rispetto delle disposizioni che può -e deve- essere aggiornato per tutto il ciclo di vita del dispositivo o della soluzione tecnica, poiché eventuali modifiche di quest'ultimi, o del contesto in cui gli stessi interagiscono per l'elaborazione dei dati, possono comportare nuovi o diversi rischi per il trattamento che vanno necessariamente considerati[11].

Tale strumento, ovviamente, dovrà essere utilizzato solo in presenza di un elemento di rischio legato alla natura, all'oggetto e alla finalità del trattamento medesimo dovendosi prevedere misure specifiche per le micro, piccole e medie imprese [12].

Tali criteri sono stati indicati dalla stessa Commissione europea nella comunicazione del 4 Novembre 2010, in cui sono stati indicati diversi casi in cui la DPIA risulta assolutamente necessaria: il trattamento di dati sensibili o in caso in cui il trattamento abbia dei rischi particolari anche in relazione alle tecnologie usate, come ad esempio la videosorveglianza.

Sarebbe opportuno, dunque, che venga fatto un ricorso alla DPIA ponderato dal bilanciamento delle due variabili del rischio e della dimensione imprenditoriale[13], ferma la valutazione negativa circa l'inopportunità di rimettere ai singoli Stati il compito di autoregolamentare il recepimento del DPIA.

Si è, infatti, già potuto riscontrare come anche lievi differenze tra gli assetti normativi di Stati membri dell'Unione pregiudichi il perseguimento dell'obiettivo finale della Commissione con l'iniziativa legislativa del Regolamento.

6. Il diritto all'oblio.

Un altro punto fondamentale che verrà disciplinato dal Regolamento Privacy è quello relativo al diritto all'oblio.

[11] Indicazioni sul possibile utilizzo del sistema della DPIA si rinvengono preliminarmente nella comunicazione della Commissione europea, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, COM (2010) 609 def., Bruxelles, 4 novembre 2010, 2.2.4 (cfr., inoltre, risoluzione *Comprehensive approach on personal data protection*, cit. *supra* nota 6), la quale sottolinea come i responsabili del trattamento di tali dati debbano effettuare un'opportuna valutazione dei dati soggetti al trattamento, specie in materia di dati sensibili. Inoltre, come accennavo, la suddetta DPIA è stata menzionata sia nel regolamento che nella direttiva di riforma del pacchetto di protezione dei dati. Fondamentale elemento da mettere in evidenza, è che la PIA potrebbe assumere un valore non solo interno, ma anche internazionale: negli accesi dibattiti tra Unione Europea e Stati Uniti, questo strumento appare conciliativo delle due realtà (cfr.: Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,* December, 2010, 34 ss., pubblicato in *http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf*).

[12] Cfr. art. 33 della proposta di regolamento.

[13] In particolare, si potrebbe prevedere l'obbligatorietà di alcune procedure di valutazione in presenza di determinati criteri normativi. Tali criteri sono stati indicati nella comunicazione della Commissione europea del 4 Novembre 2010, in cui sono stati indicati diversi casi in cui la DPIA risulta assolutamente necessaria: il trattamento di dati sensibili o in caso in cui il trattamento abbia dei rischi particolari anche in relazione alle tecnologie usate, come ad esempio la videosorveglianza.

Sul diritto all'oblio, inteso come il diritto dell'individuo a non essere più ricordato per fatti che in passato furono oggetto di cronaca ma che attualmente non rivestono più un interesse pubblico, non può non apprezzarsi l'intervento del legislatore europeo, dopo gli interventi giurisprudenziali della Corte di Giustizia sul tema, che paiono aver spostato il problema del diritto all'oblio dagli effettivi titolari delle informazioni ai motori di ricerca, ossia a quei soggetti che consentono di fatto la reperibilità dei dati.

I problemi sollevati dalla memorizzazione di dati su Internet si possono così elencare: incertezza circa la fonte dell'informazione (e, dunque, anche incertezza sull'attribuibilità ed affidabilità dell'informazione), qualità e correttezza dell'informazione e, infine, proprio la contestualizzazione dell'informazione[14].

Questi tre problemi appena elencati traspaiono chiaramente dalle motivazioni della sentenza della Corte di Giustizia UE, pronunciatasi nella causa Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos e Costeja González (sent. 13 maggio 2014, causa C-131/12)[15].

In questa pronuncia la Corte di Giustizia ha accolto la posizione dell'Avvocato generale su un particolare aspetto, ossia quello dell'assoggettamento alla direttiva dei trattamenti effettuati per le esigenze di funzionamento del motore di ricerca, avallando così la ricostruzione che fa leva sullo stretto nesso di interdipendenza tra l'indicizzazione e la fornitura di servizi pubblicitari.

Su tutti gli altri aspetti, invece, la Corte di Giustizia si muove in direzione opposta e condanna il responsabile del trattamento (il *provider*) responsabile a tutti gli effetti. Egli, salvo casi particolari, non potrà mai esimersi dal dare un riscontro positivo alle richieste volte a far sì che la ricerca compiuta impiegando il nome di una persona come parola-chiave non rimandi (e consenta, con un semplice clic, l'accesso) a pagine dove sono custoditi in maniera legittima dati di non stretta attualità, i quali, ad avviso di quella stessa persona, non dovrebbero più essere rievocati.

Qualora, infatti, il responsabile del trattamento abbia reso pubblici dati personali, è tenuto ad informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Qualora poi egli avesse autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto direttamente responsabile di tale pubblicazione.

È evidente, tuttavia, che poiché i motori di ricerca si limitano a scannerizzare ed a memorizzare una copia *cache* delle pagine *web*, per metterle a disposizione degli utenti come risposta ad una *query*, gli stessi motori di ricerca non abbiano alcuna possibilità di intervenire o modificare quella pagina.

In questo senso, è di massima evidenza come un intervento legislativo sul punto sia indispensabile al fine di evitare di comprimere l'attività dei motori di ricerca e di riversare su questi ultimi costi inappropriati. Sarebbe singolare ritenere che i soggetti che consentono agli utenti di raggiungere le informazioni e, quindi, ai titolari delle

[14] A. Palmieri, R. Pardolesi, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in Nuovi Quaderni del Foro italiano, 27 maggio 2014

[15] Con nota di A. Palmieri, R. Pardolesi, *Diritto all'oblio: il futuro dietro le spalle,* in Diritto Foro It., 2014.

pagine di ottenere un guadagno, sia in termini di notorietà che di ricavo diretto derivante dalla vendita di spazi pubblicitari sul sito internet, siano al contempo gravati dei costi di rimozione delle informazioni da loro non possedute o di gestione dei relativi contenziosi.

La proposta di Regolamento in questo senso pone espressamente in capo al titolare del trattamento dei dati l'onere di cancellare e far cancellare i dati personali non più attuali, così riportando a sistema l'interpretazione offerta dalla Corte di Giustizia che espone l'elaborazione dei motori di ricerca alla minaccia allargata di cancellazione per inattualità del dato censito, pur se ancora legittimamente presente in rete.

Una carenza della proposta di Regolamento è rinvenibile nella disposizione che rimette alla Commissione il potere di adottare i provvedimenti esecutivi nei quali specificare i criteri e le condizioni per la cancellazione dei *link* e di tutte le copie di tutti i dati personali derivanti dalla pubblicazione. Pare, invero, che anche in questo caso venga rinviato il problema dell'individuazione delle concrete modalità di esercizio del c.d. *right to be forgotten*.

Al fine di non perdere l'occasione di definire un quadro normativo unitario, nel quale le istanze di tutti gli *stakeholders* possano trovare adeguato bilanciamento, risulta essere, dunque, fondamentale provvedere a disciplinare quanto prima l'aspetto, di fatto essenziale, del *right to be forgotten* sia per la tutela degli utenti che per la posizione dei *provider*, ossia del ruolo dei motori di ricerca ai fini del suo esercizio.

Roma, 13 novembre 2014