DIritto Mercato Tecnologia

Numero 2
Anno I
Luglio/Settembre 2011

CON CONTRIBUTI DI:

Eleonora Ciccone, Michele Contartese, Annalisa De Luca, Stefania Ercolani, Francesco Graziadei, Gianluigi Magri, Davide Mula, Augusto Preta, Eugenio Prosperetti, Eleonora Sbarbaro, Francesco Soro, Andrea Stazi.

Diritto Mercato Tecnologia
www.dimt.it
ISSN (Online edition): 2239-7442

L'identità personale nel sistema delle comunicazioni elettroniche: dai social network alla normativa comunitaria

di
Francesco Soro, Annalisa De Luca

All'indomani dell'ennesimo aggiornamento delle impostazioni sulla privacy operato da Facebook, si rende necessario un ripensamento a più livelli da parte delle istituzioni in merito al significato della privacy che consenta di determinare con maggior precisione rispetto all'attuale assetto giuridico l'ambito di applicazione della normativa comunitaria in materia di trattamento di dati personali e di competenza territoriale degli organi di vigilanza da parte delle autorità europee su servizi offerti online da parte di soggetti spesso non facilmente collocabili geograficamente.
Se da una parte è indubbio che sia strettamente compito delle istituzioni influenzare la scelta su ciò che è, o può diventare, di pubblico dominio e ciò che afferisce invece alla sfera privata, non altrettanto immediato sembra essere identificare i confini del ruolo delle istituzioni. Hansen 0 esemplifica tale criticità con il rifiuto di un'azienda di processare in modo trasparente i dati personali facendo leva sul diritto concorrente alla proprietà intellettuale che l'azienda esercita, o vorrebbe esercitare, sui dati da essa detenuti a scopo commerciale. Si configura così il rischio, laddove le istituzioni non si facciano carico del compito di tracciare suddetti confini, che un soggetto privato si faccia portatore di una *public choice*.
Il termine privacy può essere interpretato da diversi punti di vista. Philips 0 utilizza la seguente suddivisione: libertà dalle intrusioni; gestione delle identità; sorveglianza; separazione pubblico/privato. La libertà da intrusioni costituisce la nozione classica di privacy ed è strettamente legata alla definizione originale offerta da Warren e Brandeis 0, i quali hanno definito la privacy come "il diritto di essere lasciato solo". Gurses e Berendt 0 pongono invece l'accento sulla "privacy come forma di occultazione", concentrandosi quindi sull'aspetto della riservatezza.
La gestione delle identità è anche la capacità di costruirsi molteplici identità sociali, ovvero – con riferimento alla definizione di privacy Westin 0 – il diritto di un individuo di "controllare, modificare, gestire ed eliminare le informazioni su loro e decidere quando, come e in quale misura tali informazioni siano comunicate ad altri". In 0, questa configura la "privacy come forma di controllo", ponendo quindi l'accento sulla sfera individuale e sul diritto di autodeterminazione degli individui in merito alla diffusione di informazioni personali. Questa accezione di privacy è accolta anche dalla Direttiva europea 95/46/CE 0, con la quale si impone il dovere di trasparenza nel trattamento dei dati personali.

D'altra parte, secondo Philips 0, la sorveglianza "... si concentra meno sui danni cagionati specificamente agli individui e più sulle pratiche di creazione e gestione della conoscenza sociale, in particolare la conoscenza di gruppi della popolazione", pertanto focalizzandosi sulla segmentazione e classificazione di gruppi all'interno di una popolazione.
Secondo Clauß et al. 0, l'insieme delle caratteristiche degli utenti che vengono registrate elettronicamente possono essere ricomprese sotto il termine "identità digitale", poiché tale insieme di attributi o caratteristiche viene utilizzato per individuare l'identità dell'utente nel contesto di uno specifico dominio. Hansen e Meissner 0, d'altra parte, forniscono una definizione più ampia del termine identità – senza la specificazione "digitale". Così ogni persona possiede una sola identità e l'identità digitale non è altro che un sottoinsieme di tale identità. Contrariamente a questa definizione, Pfitzmann e Hansen 0 la definiscono come l'insieme di attributi che potrebbe condurre ad associare un utente con la sua identità. In altre parole, ogni utente possiede identità multiple che, nel loro complesso, costituiscono la sua identità completa; tuttavia, solitamente l'utente non fornisce la propria identità completa ai *service provider* (es. un *social network*) ma solo un suo sottoinsieme costituito da un determinato numero di attributi, generalmente detto "identità parziale". Sebbene parziale, tale identità è sufficiente a rappresentare l'utente in un determinato contesto.
Il contesto definisce quali attributi personali l'utente è tenuto ad includere nella propria identità parziale. Tale contesto può essere rappresentato dai soggetti con cui si instaura un rapporto di comunicazione. Pertanto, a ciascun contesto corrisponde l'attitudine naturale degli individui a gestire la propria identità in maniera intuitiva, spontanea. Mentre un'identità (digitale) definisce esplicitamente un utente, altrettanto non si verifica necessariamente per le identità parziali. A seconda del volume e del tipo di attributi personali inclusi in un'identità parziale, l'utente può essere identificabile o rimanere nell'anonimato. Per esempio, un utente rimane anonimo in un gruppo di utenti laddove l'insieme di attributi personali che costituiscono la sua identità parziale non siano sufficienti ad identificarlo 0.
D'altra parte, la connettività costituisce una seria minaccia per il principio di autodeterminazione, permettendo a terzi di acquisire informazioni che conducono all'identificazione vera e propria dell'individuo. Soprattutto nel *social web*, che si basa precipuamente sull'utilizzo e lo scambio di dati personali, la combinazione delle differenti identità parziali – come riconosciuto anche nel rapporto di ENISA 0 – può facilitare i furti di identità.
Secondo Pfitzmann e Hansen 0 due identità parziali non sono collegabili se non è possibile stabilire se esiste una relazione fra di esse. Dal punto di vista tecnico, due identità parziali sono collegabili se un attributo personale risulti identico in entrambe le identità parziali o se una

combinazione degli attributi personali permette di stabilire una relazione 0.
La difficoltà nell'individuare possibili minacce di connessione risiede nell'identità nascosta dell'aggressore. Soprattutto nel *social web*, dove le identità parziali sono disseminate su numerosi siti, è difficile prevedere le intenzioni dell'aggressore. Per esempio, mentre Giordano permette a Daria di accedere alla sua identità parziale 1, che non contiene informazioni che permettano di identificarlo, Daria potrebbe essere in grado di costruire un'identità parziale che contiene più informazioni parziali di quelle che Giordano aveva originariamente deciso di rendere note a Daria. Nel peggiore dei casi, Daria potrebbe rivelare l'identità di Giordano. È questa la situazione di pericolo che molti osservatori contestano ai dirigenti di Facebook con ancor più veemenza dallo scorso settembre.
Dopo aver definito i termini identità e identità parziale, passiamo a definire i "dati personali". Stando al testo della Direttiva europea 95/46/CE (c.d. Data Protection Directive), i dati personali si definiscono come "qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale"0.
La stessa fonte suddivide i dati personali in sei gruppi di attributi utili a descrivere una persona, i quali includono dati fisici, fisiologici, mentali, economici, culturali e sociali. In aggiunta, i dati relativi ad un utente identificabile permettono la diretta identificazione della persona interessata. L'Independent Centre for Privacy Protection, Schleswig-Holstein, identifica i seguenti quali attributi unici di una persona 0: sesso, nome di battesimo, cognome, data di nascita, luogo di nascita, numero del certificato di nascita, identità dei genitori, nazionalità, luogo di residenza e professione. Molti di questi attributi sono indicati nei documenti di identità e rappresentano pertanto grande valore per l'identificazione, sebbene tale valore dipenda strettamente dall'entità del gruppo in cui l'individuo cerca anonimato.
Mentre è indubbio che suddetti punti di vista sulla privacy restino validi, la definizione deve necessariamente essere estesa in modo da essere applicabile al *social web*, che intrinsecamente riguarda la condivisione di informazioni personali, investendo pertanto gli obblighi di legge, l'interesse dei *policy maker* di catturare gli input provenienti dalla società, nonché la richiesta dell'utente finale di tutela della propria privacy. In ultima istanza, si tratta di elaborare un modello multilaterale di tutela della privacy mirando ad un equilibrio tra le diverse esigenze dei diversi soggetti coinvolti.
Analizziamo dunque le direttive europee pertinenti nell'ambito della privacy al fine di individuare le radici normative per il trattamento dei dati personali, in particolare nel campo dei *social media* – in particolare,

la Direttiva Protezione Dati 95/46/CE 0 e la Direttiva relativa alla vita e alle comunicazioni elettroniche 2002/58/CE 0, che contiene norme speciali per l'elaborazione dati nelle comunicazioni elettroniche. La prima direttiva è stata adottata dopo l'approvazione nell'ottobre 1995 da parte del Parlamento europeo di una Risoluzione per regolare il trattamento dei dati personali, ma ci sono voluti diversi anni affinché gli Stati membri recepissero e dessero attuazione alla direttiva nell'ambito del diritto nazionale. La Germania, ad esempio, non l'ha recepita prima del 2001, il che mostra chiaramente la complessità della legge che regola il trattamento dei dati personali.
Le due direttive sopra menzionate sono integrate da pubblicazioni di *follow-up* elaborate dal Gruppo di lavoro sulla protezione dei dati del Commissario europeo per la protezione dei dati (c.d. Article 29 Data Protection Working Party poiché istituito dall'art. 29 della Direttiva del '95), un organo indipendente di consulenza chiamato ad offrire soluzioni a problemi pratici e a fornire linee guida per l'applicazione delle direttive di cui sopra 0.
La normativa europea è poi stata integrata con Direttiva 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione 0, dal Regolamento CE n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori 0 e, da ultimo, dalla Direttiva 2009/136/CE recante modifiche alle precedenti 0, sebbene nel 2008 il Consiglio europeo sia intervenuto con una Decisione Quadro – la 2008/977/JHA – sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale 0.
Come anticipato, la locuzione "dati personali" comprende tutte le informazioni riguardanti una persona fisica identificata o identificabile. Una persona è identificabile, ad esempio, quando utilizza un identificativo (ID) univoco ovvero uno o più elementi specifici della propria identità fisica, economica, culturale o sociale. Pertanto, la Direttiva si concentra esclusivamente sulle persone fisiche.
La Direttiva non fa distinzione tra trattamento dei dati automatico e manuale; si dice, pertanto, che essa sia agnostica rispetto alla tecnologia (*technology agnostic*). Ci sono alcune eccezioni nel trattamento dei dati personali per cui non è previsto il rispetto delle disposizioni dettate dalla Direttiva, ovvero le informazioni raccolte nel perseguimento della tutela e della sicurezza nazionale.
I principali capisaldi della Direttiva possono essere riassunti come segue: 1) legalità; 2) consenso; 3) limitazione delle finalità; 4) necessità; 5) trasparenza; 6) sicurezza dei dati; 7) controllo. Se da una parte suddetti aspetti forniscono una prima panoramica su come applicare la direttiva, corre tuttavia l'obbligo di approfondire ulteriormente ciascuno di essi. Infatti, la Direttiva 95/46/CE è stata adottata nel 1995, un periodo in cui il World Wide Web ha iniziato a guadagnare slancio, ma i termini quali web 2.0 e *social web* erano ancora sconosciuti. Ciò solleva

la questione se la Direttiva sia applicabile a questi nuovi concetti, che si affidano pesantemente la partecipazione degli utenti e la contribuzione di questi ultimi con i propri dati personali.
La legittimità della domanda è sostenuta dalla moltitudine di pubblicazioni del Data Protection Working Group, di diversi progetti europei correlati (come PrimeLife 0) e altre pubblicazioni scientifiche (tuttavia per lo più incentrate specificamente sui *social network* e sull'aspetto tecnologico legato alla salvaguardia dei dati personali, piuttosto che sull'aspetto normativo). Del resto, l'applicazione della direttiva non è un compito banale, poiché non esiste una definizione coerente dei termini *social web* e *social media*, la cui evoluzione, associata all'invenzione costante di nuove tecnologie e applicazioni, rende ancor più arduo l'ambizioso compito. E del resto, la normativa europea sulla protezione dei dati non risulta aggiornata sufficientemente spesso per rimanere al passo con tale evoluzione del *social web*, causando disambiguità e lasciando spazio a pericolose interpretazioni, quanto meno per il rischio che si discostino dalla volontà del legislatore europeo. Così Garrie et al. 0 propongono che il Data Protection Working Group si riunisca a cadenza regolare per rivalutare l'attuale quadro normativo di regolamentazione e per offrire adeguate *policy recommendations*.
Il Data Protection Working Group pone l'accento sulle questioni di attualità legate alla privacy soprattutto per quanto riguarda i *social network* 0. In particolare, è oggetto di dibattito la capacità dei *service provider* di creare facilmente profili di grandi dimensioni e di renderli fondamento del loro modello di business. Per esempio, l'accesso a tali dati può essere venduto a terzi per permettere forme di pubblicità personalizzata.
La ricerca che si è occupata dell'applicabilità della Direttiva, come anticipato, è stata condotta nell'ambito del progetto PrimeLife 0. In esso gli autori concludono che la normativa europea si applica anche agli operatori con sede legale al di fuori dell'Unione Europea solo al ricorrere di almeno una di due condizioni: "1) se il trattamento dei dati personali avviene all'interno del SEE (SEE sta per Spazio Economico Europeo); 2) se il trattamento dei dati avviene al di fuori del SEE ma avvalendosi di attrezzatura con base all'interno del SEE". In quest'ottica, i *cookie* ("frammenti di testo inviati da un server ad un *web client* (di solito un browser) e poi rispediti dal client al server - senza subire modifiche - ogni volta il client accede allo stesso server 0") sono visti come attrezzatura poiché comunemente usati per tracciare un utente nel corso di più sessioni e per memorizzare informazioni aggiuntive lato *client*. Poiché i *cookie* vengono memorizzati nei confronti di *client* cittadini dell'UE, i fornitori di servizi utilizzano apparecchiature all'interno dell'Unione europea. Analogamente, il Data Protection Working Group 0 conclude che la Direttiva trovi quasi sempre applicazione nei confronti dei *provider* di *social network*, benché la loro sede principale si trovi al di fuori dell'Unione europea.

I fornitori del *social web* sono pertanto chiamati a rispettare pienamente i sette requisiti sopra elencati. In tal modo la sicurezza dei dati è di fondamentale importanza per stabilire l'affidabilità delle applicazioni *social web*. I fornitori di servizi sono quindi chiamati a prendere appropriate misure tecniche e organizzative di sicurezza, sia nella fase di progettazione di un nuovo sistema informativo (che elabora dati personali) che nella fase di funzionamento. Sintetizzando i risultati, i fornitori di servizi devono 0:
informare l'utente circa lo scopo di elaborazione dati, come ad esempio per pubblicità personalizzata, la condivisione dei dati con terzi e il trattamento dei dati altamente sensibili;
fornire meccanismi per ridurre il rischio che terzi possano accedere ai dati personali. Inoltre i dati personali devono essere esclusi dall'indicizzazione operata dai motori di ricerca;
offrire modalità semplici per cancellare completamente i propri dati;
richiedere il consenso della persona interessata a includere i riferimenti alla propria persona (per esempio per il "*tag*" di foto su Facebook);
informare l'utente su eventuali rischi legati alla violazione della privacy;
pubblicare dati personali sensibili solo se la persona interessata abbia esplicitamente dato il suo consenso.
Analogamente il Working Group afferma i seguenti diritti della persona interessata: utilizzare un servizio specifico nel *social web* senza ricorrere all'utilizzo di dati personali, ma ricorrendo a uno pseudonimo; veder garantita, da parte del fornitore di servizi, la conformità dei diritti del soggetto interessato (sia che si tratti di soci del servizio che a soggetti non ne siano soci) con gli articoli 12 e 14 della Direttiva Protezione Dati.
Il 4 novembre 2010 la Commissione europea ha pubblicato una bozza di comunicazione con la quale proponeva "un approccio globale alla protezione dei dati all'interno dell'Unione europea", al fine di modernizzare il sistema giuridico europeo per la protezione dei dati personali. La comunicazione è il risultato della revisione effettuata dalla Commissione del quadro giuridico attuale, iniziato con una conferenza di alto livello tenutasi a Bruxelles nel maggio 2009 e seguita da una consultazione pubblica e ulteriori consultazioni mirate con gli *stakeholder* tenutesi nel corso di tutto il 2010. Benché la Commissione ritenga che i principi fondamentali della Direttiva siano ancora validi, la Comunicazione riconosce che l'attuale quadro giuridico per la protezione dei dati nell'Unione europea non sia più in grado di affrontare le sfide poste dai rapidi sviluppi tecnologici e dalla globalizzazione. La comunicazione individuale pone poi sfide specifiche, compresa l'esigenza di:
chiarire e specificare l'applicazione dei principi di protezione dei dati alle nuove tecnologie (ad esempio, al *social web* e al *cloud computing*);
migliorare l'armonizzazione tra le leggi di protezione dei dati fra Stati membri dell'UE;
semplificare il trasferimento transfrontaliero di dati, rendendolo meno gravoso;

aumentare l'effettiva applicazione da parte delle autorità nazionali preposte alla protezione dei dati.
La Comunicazione dovrà servire come base per ulteriori future discussioni e valutazioni; in particolare, la Commissione ha invitato le parti interessate e il pubblico a commentare le proposte entro il 15 gennaio 2011, con l'intenzione di raccogliere spunti di riforma normative e di valutare la necessità di adeguare altri strumenti giuridici al nuovo quadro di protezione dei dati.
In conclusione, i risultati indicano che esiste un divario tra la direttiva 95/46/CE e la rapida evoluzione del web sociale. Mentre la direttiva è tecnologicamente agnostica, essa trova applicazione nell'ambito delle recenti tecnologie, come il *social web*, e dei problemi di privacy a esse connessi. Tuttavia, mentre la direttiva fornisce una solida base per proteggere la privacy dell'utente negli Stati membri dell'Unione europea, lo scambio di dati con i paesi terzi non risulta sufficientemente regolamentato, generando implicazioni legate alla privacy, la cui protezione al di fuori dell'Unione europea non può essere garantita. La Commissione europea non ha mancato di riconoscere le sfide attuali, pubblicando, quale documento per la consultazione, la bozza della Comunicazione per modernizzare l'applicazione dei principi di protezione dei dati alle nuove tecnologie. Duecentottantotto sono i documenti pervenuti alla Commissione da parte di pubbliche amministrazioni, organizzazioni e liberi cittadini, ma del testo definitivo della Comunicazione ad oggi ancora non si conoscono i risultati.

_____
Note:
ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 5/2009 on online social networking, June 2009.
CAMENISCH, J., ET AL, Privacy and Identity Management for Everyone, 2005.
CARTER, V., *Privacy Please: A Privacy Curriculum Taxonomy (PCT) for the Era of Personal Intelligence.* College Teaching Methods & Styles Journal. 2007. Third Quarter 2007: 3 (3).
CLAUß, S., KESDOGAN, D., KOLSH, T., Privacy Enhancing Identity Management: ProtectionAgainst Re-identification and Profiling, 2005.
ENISAPosition Paper, Security Issues and Recommendations for Online Social Networks, 2007.
EUROPEAN UNION, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Official Journal L 350 , 30/12/2008 P. 0060 – 0071, 2008.
EUROPEAN UNION, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002.

EUROPEAN UNION, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995.
FISCHER-HÜBNER, S., Hedbom, H., Karlstad, U. Privacy and Identity Management for Europe - Framework V3. March 2008
GARRIE, D.B., DUFFY-LEWIS, M., WONG, R., GILLESPIE, R.L., Data Protection: The Challenges Facing Social Networking, 2010. In: Brigham International Law and Management Review 6 (2010), May, S. 127–152.
GURSES, S., BERENDT, B., The Social Web and Privacy: Practices Reciprocity and Conflict Detection in Social Networks, 2009.
HANSEN, M., User-controlled identity management: the key to the future of privacy, 2008.
HANSEN, M., MEISSNER, S., Verkettung digitaler Identitäten, 2007.
INDEPENDENT CENTRE FOR PRIVACY PROTECTION and Studio Notarile Genghini, Identity Management Systems, Identification and Comparison Study, 2003
KOBSA, A., Tailoring Privacy to Users' Needs, Department of Information and Computer Science, In: M. Bauer, P.J. Gmytrasiewicz, and J. Vassileva (eds.): UM 2001, Springer-Verlag Berlin Heidelberg, pp. 303–313, 2001.
PHILLIPS, D.J., Privacy policy and PETs – the influence of policy regimes on the development and social implications of privacy enhancing technologies, 2004.
PFITZMANN, A., HANSEN, M., Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, 2008.
PRIMELIFE, Privacy Enabled Communities. Deliverable D1.2.1, April 2010.
STAZI, A., La comunicazione elettronica delle informazioni, la loro utilizzazione commerciale e le esigenze di tutela della privacy e sicurezza dei dati, Diritto Mercato Tecnologia, 2011.
UNIONE EUROPEA, Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, 2009.
UNIONE EUROPEA, Direttiva 2006/24/CE del Parlamento europeo e del Consiglio riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, 2006.
UNIONE EUROPEA, Regolamento CE n. 2006/2004 del Parlamento europeo e del Consiglio del 27 ottobre 2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela

i consumatori («Regolamento sulla cooperazione per la tutela dei consumatori»), 2004.
WARREN, S., BRANDEIS, L., The right to privacy, 1890.
WESTIN, A.F., Privacy and Freedom, 1967.
WIKIPEDIA, voce: "cookie" [disponibile online] http://it.wikipedia.org/wiki/Cookie [ultimo accesso 6 ottobre 2011]
WONG, R., SAVIRIMUTHU, J., All or nothing: this is the question?: The application of Art. (2) Data Protection Directive 95/46/EC to the Internet, 2008. In: John Marshall Journal of Computer & Information Law 2 (2008), S. 241– 266.