SOCIAL NETWORK: IL IL GARANTE PRIVACY HA PREPARATO UNA GUIDA

Fiammetta Malagoli

Il Garante della privacy ha dato alle stampe una guida, che si può veramente considerare uno specchio dei nostri tempi, intitolata “Social network: attenzione agli effetti collaterali”. La guida ha lo scopo di tutelare la privacy nell’ ambito delle reti sociali (Facebook, MySpace, ecc.). E’ di un agile vademecum che ha il fine di rendere consapevoli gli utilizzatori di *social network* dei rischi che si corrono nell’ uso improprio di tali nuovi strumenti, uso che può esporre sé stessi e la propria famiglia a spiacevoli inconvenienti, conseguenti al fatto che i dati personali, e con essi anche le fotografie ed i video digitali, vengono resi disponibili indistintamente al pubblico e in modo globale.

Le premesse della guida si trovano nella 30ma Conferenza internazionale delle Autorità di protezione dei dati, che si è tenuta a Strasburgo dal 15 al 17 ottobre 2008. In quell’ occasione le varie Autorità constatavano la grande diffusione, senza precedenti, dei servizi di *social network*, che porta con sé il rischio per chi partecipa di perdere il controllo dell’ utilizzo dei propri dati, una volta che gli stessi sono stati pubblicati nella rete. Infatti, mentre l’ utente ha generalmente l’ impressione di condividere le informazioni che lo riguardano con un numero, sia pure a volte allargato, di amici, nella realtà, i dati possono raggiungere l’ intera comunità degli abbonati al servizio, che, in certi casi, possono diventare addirittura diversi milioni.

In questo modo, i dati personali possono essere copiati anche da terzi ed essere impropriamente utilizzati per costruire profili personali o per essere ripubblicati altrove. Uno degli esempi emersi in occasione della Conferenza delle Autorità di protezione dei dati personali è costituito dalla prassi invalsa presso molti uffici del personale di varie aziende di ricercare i profili-utente dei candidati all’ assunzione o dei singoli dipendenti.

I dati pubblicati su un *social network* possono, poi, essere riutilizzati, ad esempio, per finalità di marketing da parte degli stessi fornitori di servizi di reti sociali per l’ invio di messaggi mirati.

La cancellazione dei dati è spesso difficilissima da ottenere, praticamente impossibile, una volta che i dati si siano diffusi attraverso il *web*, non essendo sufficiente la cancellazione dal sito originario, perché possono esistere copie in mano a soggetti terzi.

Un ulteriore grave problema è costituito dal rischio di furti di identità ad opera di terzi non autorizzati, favorito dalla disponibilità dei dati personali contenuti nei profili-utente.

Che cosa è un servizio di *social network*? Il manuale predisposto dal Garante della privacy lo definisce come una “piazza virtuale”, cioè un luogo “in cui via Internet ci si ritrova portando con sé e *condividendo* con altri fotografie, filmati, pensieri, indirizzi di amici e tanto altro”. Quindi, l’ aspetto di primaria importanza è costituito dalla “condivisione”.

Questo falso senso di intimità o di condividere con una piccola comunità di soggetti affini (amici, familiari, compagni di scuola, ecc.) spesso spinge gli utenti ad esporre troppo la propria vita privata, rivelando informazioni strettamente personali.

Nel capitolo”Avviso ai naviganti”, il Garante ricorda che, quando si inseriscono dei dati personali su un sito, se ne perde il controllo. Quando si esce da un sito di *social network*, spesso è consentito solo di “disattivare” il proprio profilo, ma non di “cancellarlo”. I dati immessi, quindi, possono rimanere conservati nel *server*. Tra l’ altro, poiché spesso i siti dei *social network* hanno sede all’ estero, come i loro *server*, non sempre si è tutelati dalle leggi italiane o da quelle europee.

Il Garante consiglia, pertanto, di riflettere bene prima di immettere i propri dati personali *on-line*, evitando di inserire quelli che non si vuole che vengano diffusi. Bisogna, poi, pensare anche che, quando si introduce la fotografia di un amico o di un familiare o comunque di un’ altra persona e

quando si “tagga” (cioè si inserisce il nome e cognome sulla fotografia), si viola la privacy, a meno che non si sia ottenuto il consenso dell’ interessato.
Generalmente le aziende che gestiscono i *social network* si finanziano vendendo pubblicità mirate. Esse analizzano il profilo, le abitudini e gli interessi dei propri utenti e rivendono le informazioni a chi ne ha bisogno.
L’ Autorità Garante, inoltre, richiama l’ attenzione sui furti di identità, con la conseguenza che può capitare che la propria identità sia gestita *on-line* da altri, che hanno carpito le informazioni raccolte nei profili immessi dall’ utente. La data ed il luogo di nascita sono sufficienti per ricavare il codice fiscale. Altre informazioni possono essere utilizzate dai malintenzionati per risalire al conto in banca di un utente o al suo nome o alla sua password.
Nel capitolo “Ti sei mai chiesto?” sono raggruppate una serie di domande, divise per destinatari (ragazzi/e, genitori, persone che cercano un lavoro, utenti “esperti”, professionisti), da porsi prima di pubblicare su Internet i propri dati personali, le informazioni sulla propria vita o le notizie su altre persone.
Il capitolo “Consigli per un uso consapevole” raccoglie una sorta di decalogo, che permette di tenere sotto controllo i pericoli.
Il primo consiglio riguarda l’ “autogoverno”, ossia l’ opportunità di riflettere bene prima di pubblicare un dato personale. Segue, poi, il rispetto degli altri e la necessità di non inserire informazioni e immagini di altri soggetti senza prima averne ottenuto il consenso. Bisogna ricordare che le informazioni e le fotografie possono riemergere anche a distanza di anni, con la complicità dei motori di ricerca. Buona norma è quella di non usare la stessa *login* e la stessa *password* già utilizzata per altri siti *web*, per la posta elettronica, per la gestione del conto bancario *on-line*. E’ saggio creare pseudonimi diversi in ciascuna rete alla quale si partecipa e non inserire nel *nickname* la data di nascita o altre informazioni personali. E’ opportuno informarsi su chi gestisce il servizio di *social network* e su quali garanzie offre rispetto al trattamento dei dati personali, cercando le informazioni sull’ argomento fornite sotto la voce “privacy” o “privacy policy”. Inoltre, bisogna limitare al massimo le informazioni introdotte, soprattutto per quanto riguarda la reperibilità dei dati da parte dei motori di ricerca. A tale proposito, devono essere controllati come sono impostati i livelli di privacy del proprio profilo, ovvero chi può contattare l’ utente, chi può leggere quello che egli scrive, chi può inserire commenti sulle sue pagine, che diritti hanno gli utenti dei gruppi ai quali si appartiene.
Nei consigli per l’ uso, il Garante richiama l’ attenzione sul fatto che non sempre si parla, si “chatta” e si condividono le informazioni con chi si crede. Molto spesso vengono create false identità per gioco, per dispetto o per carpire informazioni riservate.
Se non si desidera ricevere pubblicità, bisogna ricordarsi di rifiutare il consenso all’ utilizzo dei dati per attività mirate di pubblicità, promozioni e marketing.
Infine, l’ Autorità Garante suggerisce di leggere con attenzione il contratto e le condizioni d’ uso che si accettano quando ci si iscrive ad un *network*, controllando anche le modifiche che vengono introdotte unilateralmente dall’ azienda, verificando di poter recedere facilmente dal servizio e di poter cancellare tutte le informazioni pubblicate sulla propria identità.
Il vademecum si conclude con il capitolo dedicato a “Il gergo della rete”, dove viene dato spazio a definizioni non tecniche dei termini informatici, ma anche delle espressioni gergali che si incontrano più facilmente nella rete.
Così si spiega che “bannare/bandire” costituisce l’ atto che l’ amministratore di un sito o di un servizio *on-line* effettua per vietare l’ accesso ad un certo utente, che non ha rispettato le regole di comportamento definite all’ interno del sito. Si viene “taggati” quando qualcuno ha attribuito il nostro nome/cognome ad un volto presente in una fotografia messa *on-line*. Si “manda un poke” (o si “poka”) quando si vuole inviare l’ equivalente digitale di uno squillo telefonico fatto ad un amico per attirarne l’ attenzione. “Postare” significa pubblicare un messaggio, non necessariamente di solo testo, all’ interno di un *newsgroup*, di un forum, di una bacheca *on-line*.

Dalle definizioni apprendiamo anche che esiste il “cyberbullismo”, costituito da atti di molestia posti in essere utilizzando strumenti elettronici, cosa che generalmente avviene caricando video o fotografie offensive su Internet o violando l’ identità digitale di una persona su un sito di *social network*.
La Conferenza delle Autorità di protezione dei dati personali ha anche raccolto una serie di raccomandazioni rivolte ai fornitori di servizi di *social network*, che devono informare gli utenti in modo comprensibile sulle conseguenze derivanti dalla pubblicazione di dati personali in un profilo e sulla possibilità che soggetti terzi (anche legittimati, come le forze dell’ ordine) accedano legalmente a tali dati.
Sempre secondo il *panel* di Garanti riuniti a Strasburgo, i fornitori devono consentire agli utenti di limitare la visibilità dell’ intero profilo e dei singoli dati ivi contenuti o ottenibili attraverso funzioni di ricerca messe a disposizione della comunità.
Un’ altra prescrizione rivolta ai fornitori di servizi di *social network* consiste nel prevedere impostazioni di *default* tali da favorire la privacy degli utenti, sul presupposto che solo una minoranza degli utenti che aderiscono ad un determinato servizio si preoccupa di modificare tali impostazioni.
I fornitori, poi, devono adottare le misure adatte ad impedire che soggetti terzi possano raccogliere in massa i dati contenuti nei profili-utente, attraverso dispositivi di *spidering*, o scaricare oppure raccogliere tali dati.
I fornitori, infine, devono fare in modo che i dati relativi agli utenti siano navigabili da parte dei motori di ricerca solo con il previo consenso espresso ed informato da parte del singolo utente.

BOX NORMATIVO:

- Risoluzione sulla tutela della privacy nei servizi di social network, 30ma Conferenza internazionale delle Autorità di protezione dei dati, Strasburgo, 15-17 ottobre 2008.
- “Social network: attenzione agli effetti collaterali”.