

Un codice su misura per i «social network»

di Alberto M. Gambino e Andrea Stazi

Il Sole 24 Ore, 21 giugno 2009

Nei giorni scorsi il Garante *privacy* ha pubblicato una guida per aiutare gli utenti a usare in modo consapevole i c.d. *social network* (Facebook, MySpace, etc.), che rappresentano ormai uno strumento di comunicazione sempre più centrale nella nostra quotidianità e nelle nostre relazioni sociali e professionali.

I *social network* sono servizi che offrono agli utenti la possibilità di interagire attraverso profili personali generati autonomamente, al fine di favorire la comunicazione tra gli stessi. Sono, in altri termini, delle comunità virtuali sulla rete alle quali milioni di soggetti si iscrivono e attraverso cui gli utenti possono scambiare notizie, immagini e informazioni personali.

Dal punto di vista della tutela dei dati personali, questa tipologia di servizi rileva in quanto consente un'agevole comunicazione di dati relativi agli utenti non solo tra questi, ma anche a soggetti terzi, con le relative potenziali lesioni della *privacy* che da ciò discendono.

In particolare, vi è il rischio che gli utenti non riescano a gestire i propri dati una volta immessi nel *social network*, in quanto le informazioni non risultano di fatto essere conoscibili dai soli soggetti abilitati dall'utente. La tutela dei soggetti che usufruiscono di questi servizi è, così, di scarsa effettività, posto che anche una successiva cancellazione dei dati su richiesta dell'utente non garantisce che soggetti terzi non possano ancora utilizzare i dati precedentemente acquisiti e copiati.

In materia, dapprima erano stati emanati due documenti, rispettivamente dall'International Working Group on Data Protection in Telecommunications, «Aspetti di sicurezza degli Online Social Networks» (ottobre 2007), e dall'ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione), «Relazione e Linee-Guida sulla Privacy nei Servizi di Social Network» (marzo 2008).

Successivamente, la Conferenza Internazionale delle Autorità per la protezione dei dati e della *privacy* ha ritenuto opportuno intervenire sul tema con una specifica «Risoluzione sulla tutela della *privacy* nei servizi di social network», adottata a ottobre 2008, in cui sono contenute un insieme di raccomandazioni rivolte sia agli utenti sia ai gestori di tali servizi.

Per quanto riguarda gli utenti, oltre a riconoscersi un diritto all'educazione alla tutela dei propri dati personali da parte dei gestori dei *social network*, dei governi e delle autorità garanti, si fa espresso richiamo all'attenzione che essi devono porre nel momento in cui valutano quali informazioni pubblicare. Gli utenti devono, infatti, tenere presente che i dati pubblicati in un tempo determinato potrebbero riemergere in momenti successivi, anche e soprattutto in contesti differenti, ad esempio nell'ambito lavorativo.

Volto a tutelare la sfera privata dei minori è, poi, il richiamo degli stessi a non indicare i contatti personali su questi spazi aperti, al fine di evitare che possano verificarsi situazioni di lesione della loro sfera personale.

Allo stesso modo, si ricorda come gli utenti abbiano l'obbligo di rispettare la *privacy* altrui, compreso il necessario consenso alla pubblicazione di foto raffiguranti soggetti terzi.

Ai fornitori dei servizi di *social network*, poi, viene fatto esplicito richiamo al rispetto della normativa vigente in tema di tutela dei dati personali, prevedendo inoltre la possibilità di affidarsi ad attività di consultazione con le autorità garanti dei Paesi in cui operano. Agli obblighi già imposti dalla legge si aggiunge quello per cui le informazioni fornite, in tema di modalità di trattamento, devono essere contestualizzate rispetto alla peculiare realtà che il *social network* rappresenta.

Obbligo dei fornitori è, inoltre, quello di vigilare sulle modalità con cui i dati dei propri utenti sono utilizzati dai terzi, attribuendo ai primi la facoltà di decidere quali dati rendere pubblici e quali visualizzabili ai soli conoscenti. In relazione all'utilizzo che terzi possono fare dei dati

acquisiti, si prevede che i fornitori debbano predisporre dei meccanismi di consenso improntati all'*opt-out*, per quanto riguarda i dati non sensibili, ed all'*opt-in* per i dati di natura sensibile contenuti nel profilo (ad esempio relativi ad opinioni politiche o all'orientamento sessuale) nonché rispetto ai dati di traffico. Al riguardo, può aggiungersi che i *social network* operanti nel nostro Paese dovranno predisporre soltanto forme di consenso improntate all'*opt-in*, dato che il Codice *privacy* richiede appunto questa forma di consenso.

Ancora, si prevede che le impostazioni iniziali, raramente modificate dagli utenti, siano volte a garantire la più assoluta tutela dei dati personali degli stessi, con limiti ancora più stringenti per i profili degli utenti minorenni.

Deve essere, poi, garantita la possibilità di utilizzare pseudonimi, consigliando agli utenti l'esercizio di questa opzione.

Infine, dati i peculiari rischi per la riservatezza insiti nei *social network*, gli standard di sicurezza adottati devono essere più stringenti, volti a garantire che soggetti terzi non possano scaricare o illecitamente sottrarre i dati, e la loro adozione ed aggiornamento all'evoluzione delle tecnologie devono essere periodicamente certificati. Nell'ambito delle tecnologie di sicurezza, in particolare, rientra l'obbligo di una completa cancellazione dei dati degli utenti, là dove questi decidano di abbandonare il *social network*.