

PRIVACY E SOCIAL NETWORK

Youtube, MySpace, Facebook, LinkedIn sono soltanto i nomi di alcune delle più note piattaforme di social network, un fenomeno socio-tecnologico di grande interesse, contraddistinto da elevatissimi tassi di crescita degli utenti.

Ma perchè queste piattaforme riscuotono così tanto successo?

E, soprattutto, quali rischi presentano per la sicurezza e la riservatezza dei nostri dati personali?

Diversi sono i fattori che influenzano il successo dei social network: la possibilità di instaurare nuove relazioni ed interagire con individui anche molto distanti da noi, la presenza di strumenti ed infrastrutture che facilitano la collaborazione online, l'idoneità a supportare la nascita e lo sviluppo di nuove iniziative e relazioni di business, il senso di intimità nelle relazioni tra gli utenti, la garanzia per gli utenti di esercitare un certo controllo sui dati generati.

D'altra parte, come sempre accade, questi vantaggi hanno anche un rovescio della medaglia: proprio a causa del falso senso di intimità, gli utenti di queste reti manifestano la propensione a rivelare informazioni personali con più facilità rispetto a ciò che accade in una relazione tradizionale, dimostrandosi nel contempo poco selettivi nella scelta delle persone con le quali allacciare nuovi contatti.

I social network stanno inoltre vivendo un periodo di intenso sviluppo commerciale, dominato dalla necessità di catturare l'attenzione e l'interesse di nuovi utenti: questo si traduce, spesso, in una scarsa attenzione verso le **problematiche relative alla sicurezza ed alla privacy**. Infine molti degli aspetti che andremo ad analizzare non risultano adeguatamente regolamentati nell'ambito delle normative comunitarie e nazionali, emanate in periodi in cui il fenomeno era ancora poco noto.

Partendo da una ricerca dell'Enisa (agenzia europea per la sicurezza delle reti e delle informazioni), i principali rischi che, allo stato attuale, le piattaforme di social network pongono con riferimento ai dati personali degli utenti possono essere classificati in:

- rischi relativi alla riservatezza dei dati;
- rischi concernenti le identità digitali;
- rischi di natura tecnologica;
- rischi di natura sociale.

Ci soffermiamo sui rischi del primo tipo che, generalmente, hanno come presupposti la mancanza, la scarsa trasparenza o l'ambiguità delle politiche di trattamento dei dati e delle condizioni di utilizzo dei servizi, ma anche la possibilità di associare immagini ai profili oppure di etichettare le immagini con particolari metadati.

In questo contesto esistono dunque delle pericolosità specifiche:

- creazione di dossier digitali ed aggregazione di dati secondari;

- tecniche di riconoscimento facciale;
- content-based image retrieval;
- metadati associati o relativi alle immagini;
- problemi nella cancellazione dei dati degli utenti.

Sul primo punto c'è poco da aggiungere salvo che chiunque abbia accesso ad un qualsiasi servizio (l'accesso è libero, basta registrarsi, ed i controlli previsti in fase di registrazione sono spesso carenti) può acquisire e raccogliere i dati degli utenti, all'insaputa di questi ultimi, ed utilizzarli per le finalità più disparate (spam, pubblicità, attacchi diretti alla persona, discriminazione, ecc....) che, raramente, corrispondono a quelle per le quali è stato prestato il consenso.

Questo inconveniente non può ritenersi superato nemmeno in virtù dei tanto sbandierati controlli di accesso, sia perchè a volte i dati personali, apparentemente non visibili, risultano accessibili mediante una semplice ricerca, sia per la debolezza intrinseca di molte impostazioni predefinite (pochi utenti si preoccupano di modificarle !), sia perchè, in realtà, è molto facile diventare "amici" di tutti ed avere così accesso ai dati. Considerazioni analoghe le possiamo fare anche per i dati di natura, per così dire, secondaria (indirizzi ip, data e durata delle connessioni, profili visitati, messaggi scambiati, ecc...): questi sono di regola accessibili ai fornitori per asserite finalità miglioramento dei servizi ma, in realtà, non esistono di fatto adeguate garanzie di protezione e, soprattutto, di trattamento per le finalità consentite.

In relazione al secondo punto, l'enorme progresso tecnico raggiunto nel campo degli algoritmi rende tutt'altro che teorico il rischio di una correlazione tra i profili, di cui gli utenti sono spesso titolari su servizi o piattaforme differenti, proprio per effetto del riconoscimento delle relative immagini (a tale proposito sembra che Google abbia già integrato nella sua ricerca immagini delle tecniche di riconoscimento facciale; vedi questo [esempio su Albert Einstein](#)). Lo stesso livello di rischio deriva dalla possibilità di utilizzare tecniche di content-based image recognition (CBIR), originariamente sviluppate nel settore della digital forensic, per dedurre informazioni utili alla geolocalizzazione degli utenti attraverso il riconoscimento delle caratteristiche degli oggetti o dei luoghi raffigurati nelle immagini associate ai profili.

La questione dei metadati abbraccia due evenienze diverse: da un lato c'è l'eventualità, offerta da alcune piattaforme, di associare alle immagini delle etichette contenenti informazioni personali relative alla persona ritratta (nome, cognome, indirizzo di posta elettronica, ecc...), senza prima aver ricevuto il consenso da parte di quest'ultima.

L'inclusione, invece, di particolari metadati nelle immagini digitali che vengono caricate sulle piattaforme, in particolare il numero seriale della fotocamera, può costituire una minaccia per la privacy dell'utente a causa della associazione con i dati relativi al suo indirizzo riportati nella cartolina di

registrazione

della

garanzia.

Infine una ulteriore questione da non sottovalutare è quella relativa alla eventuale cancellazione dal servizio: raramente, infatti, l'eliminazione dei dati principali si accompagna ad una completa rimozione di tutti i contenuti generati dall'utente (post, commenti, contenuti audio-video, ecc...).

Questa ambiguità è ulteriormente esasperata quando, a fronte di una richiesta di cancellazione, c'è soltanto una disattivazione del profilo, con conseguente mantenimento di una copia "nascosta" dei dati: entrambe le ipotesi costituiscono una violazione palese della direttiva 95/46/CE essendo gli individui privati di un mezzo efficace con il quale controllare la diffusione dei propri dati.

30^{ma} Conferenza internazionale delle Autorità di protezione dei dati Stasburgo, 15 - 17 ottobre 2008

Risoluzione sulla tutela della privacy nei servizi di social network

Autorità proponente: Autorità per la protezione dei dati e l'accesso alle informazioni dello Stato di Berlino – Germania

Co-sponsor:

Commission nationale de l'informatique et des libertés (CNIL) – Francia
Autorità federale per la protezione dei dati e l'accesso alle informazioni – Germania

Garante per la protezione dei dati personali – Italia
Autorità per la privacy – Nuova Zelanda
Autorità federale per la protezione dei dati e le informazioni – Svizzera

Risoluzione

I servizi di social network sono divenuti estremamente popolari negli ultimi anni. Fra l'altro, si tratta di servizi che offrono agli abbonati la possibilità di interagire attraverso profili personali generati autonomamente, il che favorisce la comunicazione di dati personali relativi agli abbonati, ma anche a soggetti terzi, in una misura che non ha precedenti. I servizi di social network offrono una gamma del tutto nuova di opportunità comunicative e di interazione in tempo reale attraverso ogni possibile tipologia di informazioni, ma l'utilizzo di questi servizi può comportare rischi per la privacy sia degli utenti sia di terzi. I dati personali divengono infatti disponibili pubblicamente e in modo globale, secondo schemi qualitativi e quantitativi che non hanno precedenti, anche attraverso enormi quantità di foto e video digitali.

C'è il rischio di perdere il controllo dell'utilizzo dei propri dati una volta pubblicati in rete. Il fatto che si tratti di servizi operanti attraverso una

"comunità" di utenti può far pensare che la situazione non sia molto diversa dal condividere informazioni con un gruppo di amici nel mondo reale; in realtà, le informazioni contenute nel proprio profilo possono raggiungere l'intera comunità degli abbonati al servizio – talora in numero di diversi milioni.

Attualmente non vi sono che scarse tutele rispetto alla riproduzione dei dati personali contenuti nei profili-utente; possono essere copiati da altri membri della rete, o da terzi non autorizzati esterni alla rete, e quindi venire utilizzati per costruire profili personali oppure essere ripubblicati altrove. Talora risulta assai difficile, o addirittura impossibile, ottenere la totale cancellazione dei propri dati da Internet una volta che essi siano stati pubblicati. Anche dopo la cancellazione dal sito originario (ad esempio, un servizio di social network), possono esistere copie in mano a soggetti terzi o ai fornitori del servizio di social network. Inoltre, i dati personali contenuti nei profili possono "filtrare" dalla rete se sono indicizzati da un motore di ricerca, mentre alcuni fornitori di questi servizi consentono a terzi di accedere ai dati relativi agli utenti attraverso API (interfacce di programmazione applicazioni), cosicché tali soggetti terzi sono liberi di disporre dei dati in questione.

Fra gli esempi di utilizzo ulteriore dei dati, possiamo citare la prassi invalsa presso molti uffici del personale di varie aziende di ricercare i profili-utente relativi a candidati all'assunzione o singoli dipendenti. Secondo quanto riferito dalla stampa, un terzo dei responsabili delle risorse umane ammette di utilizzare informazioni tratte da servizi di social network, ad esempio per verificare o completare le informazioni fornite dai candidati all'assunzione.

Le informazioni contenute nei profili-utente e i dati di traffico sono utilizzati anche dai fornitori di servizi di social network per l'invio di messaggi mirati di marketing ai rispettivi utenti.

E' molto probabile che in futuro si manifestino altre modalità di utilizzo dei dati contenuti nei profili-utente.

Fra gli altri rischi specifici per la privacy e la sicurezza già oggi individuati, possiamo ricordare l'incremento del rischio di furti di identità favorito dalla diffusa disponibilità dei dati personali contenuti nei profili-utente e dalla "cattura" di tali profili ad opera di terzi non autorizzati. La 30ma Conferenza Internazionale delle autorità per la protezione dei dati e della privacy ricorda che tali rischi hanno già formato oggetto di analisi nel documento "Relazione e Linee-Guida sulla Privacy nei Servizi di Social Network ("Memorandum di Roma")" adottato durante la 43ma riunione dell'International Working Group on Data Protection in Telecommunications (3-4 marzo 2008), nonché nel Position Paper n. 1 dell'ENISA dedicato a "Security Issues and Recommendations for Online Social Networks" (ottobre 2007).

Le Autorità per la protezione dei dati e della privacy riunitesi in occasione della Conferenza Internazionale sono convinte, in primo luogo, della necessità di condurre un'approfondita campagna informativa che investa tutti i soggetti pubblici e privati: dalle autorità di governo alle istituzioni scolastiche, dai

fornitori di servizi di social network alle associazioni di utenti e consumatori, nonché le stesse autorità, al fine di prevenire i molteplici rischi associati all'utilizzo dei servizi di social network.

Raccomandazioni

Tenuto conto della particolare natura dei servizi in oggetto, e dei rischi per la privacy delle persone nel breve e nel lungo periodo, la Conferenza sottopone le seguenti raccomandazioni agli utenti ed ai fornitori di servizi di social network:

Utenti dei servizi di social network

I soggetti interessati al benessere degli utenti dei servizi di social network, ivi compresi i fornitori di tali servizi, i governi, e le autorità per la protezione dei dati, dovrebbero contribuire ad educare gli utenti alla tutela dei dati personali che li riguardano, trasmettendo i messaggi di seguito indicati:

1. Pubblicazione delle informazioni

Gli utenti di servizi di social network dovrebbero valutare con attenzione se e in quale misura pubblicare dati personali in un profilo creato su tali servizi. Occorre tenere presente che le informazioni o le immagini pubblicate potrebbero riemergere in tempi successivi – ad esempio, in occasione della presentazione di una domanda d'impiego. Soprattutto, i minori dovrebbero evitare di fornire l'indirizzo o il numero telefonico di casa. Sarebbe opportuno valutare se utilizzare nel profilo un pseudonimo anziché il nome reale. Tuttavia, gli utenti devono ricordare che la tutela offerta dall'utilizzo di pseudonimi è piuttosto limitata, in quanto altri potrebbero individuare chi vi si cela dietro.

2. La privacy degli altri

Gli utenti devono rispettare la privacy altrui. Occorre particolare attenzione se si pubblicano dati personali relativi a soggetti terzi (comprese foto con o senza didascalie o etichette) senza il consenso di tali soggetti.

Fornitori dei servizi di social network

I fornitori dei servizi di social network sono tenuti ad operare nell'interesse delle persone che utilizzano i loro servizi. Oltre a rispettare la normativa in materia di protezione dei dati, dovrebbero mettere in pratica anche le raccomandazioni di seguito indicate:

1. Norme e standard in materia di privacy

I fornitori devono rispettare gli standard in materia di privacy vigenti nei Paesi ove operano. A tale scopo, dovrebbero consultarsi, se necessario, con le autorità per la protezione dei dati.

2. Informazioni relative agli utenti

I fornitori dei servizi di social network devono informare gli utenti in merito al trattamento dei dati personali che li riguardano, secondo modalità trasparenti e corrette. Inoltre, devono fornire informazioni veritiere e comprensibili sulle conseguenze derivanti dalla pubblicazione di dati personali in un profilo, nonché sugli altri rischi in materia di sicurezza e sulla possibilità che soggetti

terzi (comprese, ad esempio, le forze dell'ordine) accedano legalmente a tali dati. L'informativa deve indicare anche le modalità per una corretta gestione dei dati personali relativi a terzi che siano contenuti nei singoli profili-utente.

3. Controllo da parte degli utenti sui dati che li riguardano

E' necessario che i fornitori potenzino ulteriormente la capacità degli utenti di decidere l'utilizzo dei dati contenuti nei rispettivi profili per quanto riguarda i membri della comunità. Devono consentire agli utenti di limitare la visibilità dell'intero profilo, nonché di singoli dati contenuti nel profilo o ottenuti attraverso funzioni di ricerca messe a disposizione della comunità. Inoltre, i fornitori devono consentire agli utenti di decidere sugli utilizzi ulteriori dei dati di traffico e dei dati contenuti nei rispettivi profili – ad esempio, per quanto riguarda attività di marketing. Come minimo, devono offrire la possibilità di negare il consenso (opt-out) rispetto all'utilizzo dei dati non sensibili contenuti nel profilo, e prevedere un consenso previo (opt-in) rispetto all'utilizzo di dati di natura sensibile contenuti nel profilo (ad esempio, dati relativi ad opinioni politiche o all'orientamento sessuale) nonché rispetto ai dati di traffico.

4. Impostazioni di default orientate alla privacy

Inoltre, i fornitori devono prevedere impostazioni di default orientate a favorire la privacy degli utenti per quanto riguarda le informazioni contenute nei singoli profili. Le impostazioni di default sono essenziali ai fini della tutela della privacy; è noto come solo una minoranza degli utenti che aderiscono ad un determinato servizio si preoccupi di modificare tali impostazioni. Le impostazioni in oggetto devono essere particolarmente restrittive se il servizio di social network è destinato o rivolto a minori.

5. Sicurezza

I fornitori devono continuare a potenziare e garantire la sicurezza dei sistemi informativi, impedendo accessi abusivi ai profili-utente, utilizzando standard riconosciuti per quanto concerne la programmazione, lo sviluppo e la gestione delle rispettive applicazioni, e ricorrendo a verifiche e certificazioni indipendenti.

6. Diritti di accesso

I fornitori devono riconoscere alle persone (siano esse membri del servizio o meno) il diritto di accedere e, se necessario, apportare modifiche a tutti i dati personali detenuti dai fornitori stessi.

7. Cancellazione dei profili-utente

I fornitori devono permettere agli utenti di recedere facilmente dal servizio, cancellando il rispettivo profilo ed ogni contenuto o informazione da essi pubblicato attraverso il servizio di social network.

8. Utilizzo di pseudonimi

I fornitori devono consentire la creazione e l'utilizzo, in via opzionale, di profili basati su pseudonimi e promuovere il ricorso a tale modalità opzionale.

9. Accesso da parte di soggetti terzi

I fornitori devono prendere misure atte ad impedire che soggetti terzi possano raccogliere attraverso dispositivi di spidering e/o scaricare (o raccogliere) in massa i dati contenuti nei profili-utente.

10. Indicizzazione dei profili-utente

I fornitori devono garantire che i dati relativi agli utenti siano navigabili da parte dei motori di ricerca soltanto con il previo consenso espresso ed informato da parte del singolo utente. Deve essere prevista per default la non-indicizzazione dei profili-utente da parte dei motori di ricerca.

(* Traduzione non ufficiale

(1) "Un servizio di rete sociale (social network) consiste in via primaria nella costruzione e nella verifica di reti sociali online rivolte a comunità di soggetti che condividono interessi e attività, o che sono interessati ad esplorare gli interessi e le attività altrui [...]. Si tratta di servizi che, per la massima parte, sono gestiti attraverso il web ed offrono diverse modalità di interazione fra gli utenti [...]." Tratto da Wikipedia:

http://en.wikipedia.org/wiki/Social_network_service

Contributo del Consiglio d'Europa

Il Consiglio d'Europa ha pubblicato il contributo che porterà al prossimo Forum delle Nazioni Unite sulla Governance di Internet, organizzato dal 3 al 6 dicembre a Hyderabad, in India. Con lo slogan «Internet - una risorsa essenziale per tutti», il contributo attribuisce particolare importanza ai diritti degli utenti. Diritti che sono oggetto dell'attenzione anche delle Autorità per la privacy che si sono riunite in conferenza a Strasburgo e che hanno deciso di adottare severi provvedimenti per difendere la privacy degli internauti.

Il problema, infatti, è che i siti di social networking come Facebook e MySpace sono pieni di dati sensibili immessi dagli stessi utenti e che non di rado finiscono nei motori di ricerca. Come è accaduto alla figlia di Sarah Palin, candidata vicepresidente per i repubblicani nelle elezioni USA, la cui gravidanza doveva rimanere segreta e invece è finita su tutti i mezzi di informazione, a causa della confidenza fatta dal suo ragazzo a un amico proprio tramite Facebook.

Secondo quanto concordato dalle Autorità dei 78 paesi che si sono dati appuntamento a Strasburgo, i social network dovranno adottare misure per rendere inaccessibili ai motori di ricerca tutti i dati sensibili dei propri utenti, a meno che questi ultimi non diano il proprio assenso. In secondo luogo, i provider responsabili del funzionamento dei vari aggregatori sociali virtuali

dovranno fornire ai netizen informazioni trasparenti e approfondite sui rischi derivanti dalla diffusione dei propri dati personali e limitare la visione completa dei profili degli utenti solo ad altri utenti iscritti allo stesso social network.