Rapporto e Linee-Guida in materia di privacy nei servizi di social network

[doc. web n. 1567124]
[v. anche Comunicato stampa]

Rapporto e Linee-Guida in materia di privacy nei servizi di social network (*)
"Memorandum di Roma"
Adottato in occasione del 43mo incontro, 3-4 marzo 2008, Roma

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS

Rapporto

Il contesto
"Un servizio di social network (rete sociale) consiste nella creazione e nel controllo di reti sociali online destinate a comunità di soggetti che condividono determinati interessi e attività, ovvero intendono esplorare gli interessi e le attività di altri soggetti, necessariamente attraverso l´impiego di applicazioni software. Si tratta in maggioranza di servizi basati sull´utilizzo del web; numerose sono le modalità di interazione fra gli utenti […](1). Più specificamente, molti siti offrono strumenti per interagire con altri abbonati (sulla base di profili personali generati autonomamente)"(2).

L´avvento e la crescente popolarità dei servizi di social network segnalano un cambiamento radicale nell´accessibilità pubblica, quale ne sia il livello, dei dati personali relativi ad una grossa fetta della popolazione in tutto il mondo. Negli ultimi anni, le reti sociali hanno incontrato un favore incredibile, soprattutto fra i giovani. Tuttavia, avviene sempre più spesso che servizi di questo tipo siano offerti, ad esempio, anche a professionisti o a soggetti anziani.

Le sfide che derivano da questi servizi rappresentano, da un lato, un´altra manifestazione dei cambiamenti radicali introdotti dall´avvento di Internet negli anni ´90 dello scorso secolo, che hanno comportato l´abolizione dei vincoli spaziali e temporali per quanto concerne la pubblicazione di informazioni e comunicazioni in tempo reale nonché reso più labile la distinzione fra fornitori di servizi (autori) e utenti/consumatori (lettori).

D´altro canto, i servizi di social network sembrano mettere in discussione il concetto di spazio individuale nella sua accezione sociale. I dati personali divengono accessibili pubblicamente (e a livello globale) secondo modalità e in quantità sinora sconosciute(3); soprattutto, ciò avviene nei riguardi di un´enorme quantità di immagini e video digitali.

Per quanto concerne la privacy, una delle sfide di fondo è rappresentata probabilmente dal fatto che la maggioranza dei dati personali pubblicati attraverso servizi di questo tipo sono resi pubblici su iniziativa degli stessi utenti e in base al loro consenso. Mentre le norme "tradizionali" in materia di privacy vertono sulla definizione di regole che tutelino i cittadini dal trattamento sleale o sproporzionato dei loro dati personali da parte dei soggetti pubblici (compresi polizia e servizi segreti) e delle imprese, vi sono pochissime norme che disciplinino la pubblicazione di dati

personali su iniziativa dei singoli – anche perché ciò non ha mai rappresentato un tema di primo piano nel mondo "offline", e neppure su Internet prima dell´avvento dei servizi di social network. Inoltre, la legislazione in materia di protezione dati e privacy ha tradizionalmente previsto norme di favore per il trattamento di dati personali derivanti da fonti pubbliche.

Al contempo, siamo dinanzi ad una nuova generazione di utenti. Si tratta della prima generazione cresciuta insieme ad Internet. Questi "indigeni digitali" hanno sviluppato approcci del tutto peculiari rispetto all´utilizzo dei servizi Internet ed al concetto di privato ovvero pubblico. Inoltre, essendo in buona parte adolescenti, sono probabilmente più disposti a mettere a rischio la propria privacy rispetto agli "immigrati digitali"[(4)] con qualche anno di più. In linea di massima, sembra di poter affermare che chi è più giovane ha meno problemi a rendere pubblici dettagli anche intimi della propria vita attraverso Internet.

I legislatori, le autorità di protezione dati e i fornitori di servizi di social network si trovano ad affrontare una situazione per la quale non ci sono riscontri in passato. I servizi di social network offrono tutta una serie di nuove opportunità di comunicazione e scambio di informazioni di ogni genere, in tempo reale, ma l´utilizzo di questi servizi può comportare anche rischi per la privacy degli utenti – e di altri cittadini che non hanno mai aderito a questi servizi.

Rischi per la privacy e la sicurezza

L´ascesa dei servizi di social network è appena agli inizi. Anche se si possono già intravedere alcuni rischi associati all´offerta ed all´utilizzo di questi servizi, con ogni probabilità quella che vediamo è soltanto la punta dell´iceberg e nei prossimi anni continueranno ad emergere nuove forme di utilizzo e, quindi, nuovi rischi. Più in particolare, soggetti pubblici (compresi polizia e servizi segreti)[(5)] e privati escogiteranno nuove modalità di utilizzo dei dati personali contenuti nei profili-utente.

I rischi che sono elencati di seguito non sono che una fotografia dell´esistente, e probabilmente dovranno essere rivisti e corretti alla luce degli sviluppi dei servizi di social network.

I rischi sinora individuati in rapporto all´utilizzo di servizi di social network sono i seguenti:

Niente oblio su Internet. Il concetto di oblio non esiste su Internet. I dati, una volta pubblicati, possono rimanerci letteralmente per sempre – anche se la persona interessata li ha cancellati dal sito "originario", possono esisterne copie presso soggetti terzi; appartengono a quest´ultima categoria i servizi di archivistica e la funzione di "cache" disponibile presso un notissimo motore di ricerca. Inoltre, alcuni fornitori di servizi rifiutano di ottemperare (o non ottemperano affatto) alle richieste degli utenti di ottenere la cancellazione di dati e, soprattutto, di interi profili.

L´idea ingannevole di "comunità". Molti fornitori di servizi affermano di trasferire le strutture comunicative dal mondo "reale" al cyberspazio. Un´affermazione frequente è che non ci sarebbero problemi, per esempio, a pubblicare dati (personali) su queste piattaforme, perché è come se si condividessero informazioni con un gruppo di amici nel mondo reale. Se però si vanno ad esaminare con più attenzione alcune caratteristiche di certi servizi, si vedrà che il parallelo non regge – anche perché il concetto di "amici" nel cyberspazio può risultare assai diverso dall´idea più tradizionale di amicizia, e la comunità può essere assai estesa[(6)]. Se non si informano gli utenti in modo trasparente sulle modalità di condivisione delle informazioni contenute nei loro profili, e sugli strumenti con i quali essi possono decidere tali modalità, può avvenire che l´idea di una "comunità" descritta nei termini sopra richiamati finisca per indurli a rivelare in modo sconsiderato informazioni personali che altrimenti non si lascerebbero sfuggire. Anche i nomi dati a talune di queste piattaforme (come "MySpace") creano un´idea illusoria di privacy e riservatezza sul web.

"Gratis" non sempre significa "a costo zero". In realtà, molti dei servizi di social network fanno "pagare" gli utenti attraverso il riutilizzo dei dati contenuti nei profili personali da parte dei fornitori di servizio, ad esempio per attività (mirate) di marketing.

La raccolta di dati di traffico da parte dei fornitori di servizi di social network, i quali hanno gli strumenti tecnici per registrare ogni singolo passo dell´utente sul loro sito e, in ultima analisi, comunicare a terzi dati personali (di traffico) – compresi gli indirizzi IP, che in taluni casi possono ricordare i dati relativi all´ubicazione. Ciò può avvenire, ad esempio, per finalità pubblicitarie, anche di tipo mirato. Si osservi che in molti Paesi i dati in oggetto devono essere comunicati, a richiesta, anche alle autorità giudiziarie o di polizia e/o ai servizi di intelligence (nazionali), nonché con ogni probabilità, in base alle norme esistenti in materia di cooperazione internazionale, a soggetti stranieri.

Il bisogno crescente di finanziare i servizi e ricavare profitti può fungere da stimolo ulteriore per la raccolta, il trattamento e l´utilizzazione di dati relativi agli utenti, trattandosi dell´unico cespite patrimoniale dei fornitori di servizi di social network. I siti di social network non sono – contrariamente a quanto suggerito dal termine "social" – un servizio pubblico. D´altra parte, il web 2.0 sta "diventando adulto" e le piccole aziende informatiche gestite, in certi casi, da gruppi di studenti meno interessati all´aspetto finanziario sono sostituite sempre più spesso da grandi soggetti di respiro internazionale. Tutto questo ha cambiato in qualche misura le regole del gioco, visto che molte delle imprese di cui sopra sono quotate in borsa e subiscono una pressione fortissima da parte dei rispettivi investitori nell´ottica di realizzare e massimizzare profitti. Poiché per molti fornitori di questi servizi i dati contenuti nei profili degli utenti ed il numero di utenti esclusivi (uniti alla frequenza di utilizzo) costituiscono gli unici veri beni patrimoniali di cui dispongono, possono sorgere rischi ulteriori per quanto riguarda la raccolta, il trattamento e l´utilizzo non proporzionati dei dati personali relativi agli utenti. Si osservi che, ad oggi, molti fornitori di servizi di social network adottano il principio di esternalizzare verso gli utenti i costi relativi alla privacy(7).

Rivelare più informazioni personali di quanto si creda. Ad esempio, le foto possono trasformarsi in identificatori biometrici universali all´interno di una rete ed anche attraverso più reti. Negli ultimi anni sono migliorate in misura notevole le prestazioni dei software di riconoscimento del volto, e risultati ancora "migliori" arriveranno in futuro. Si osservi che, una volta associato un nome ad una foto, possono essere messe a rischio anche la privacy e la sicurezza di altri profili-utente, magari basati sull´uso di pseudonimi o addirittura di dati anonimi – ad esempio per quanto riguarda i profili di possibili partner, che in genere contengono una foto e informazioni personali, ma non il vero nome del singolo interessato. Inoltre, l´ENISA (l´agenzia europea per la sicurezza delle reti e delle informazioni) ha richiamato l´attenzione su una tecnologia emergente (CBIR, content-based image retrieval) che offre ulteriori opportunità di localizzare gli utenti associando gli elementi identificativi di determinati ambienti o luoghi (ad esempio, un dipinto appeso in una stanza, o un edificio visibile nell´immagine) ai dati relativi all´ubicazione contenuti in un database(8). Infine, le funzioni dette di "grafo sociale", molto diffuse presso vari servizi di social network, di fatto rivelano informazioni sui rapporti intercorrenti fra i singoli utenti.

Utilizzo improprio dei profili utente da parte di soggetti terzi. Si tratta probabilmente del rischio potenziale più grave per quanto riguarda i dati personali contenuti nei profili utente dei servizi di social network. A seconda della configurazione (di default) disponibile rispetto alla privacy e dell´utilizzo o meno di tale configurazione da parte degli utenti, nonché del livello di sicurezza offerto dal servizio, le informazioni contenute nel profilo (comprese immagini, che possono ritrarre sia il singolo interessato, sia altri soggetti) diventano accessibili, nel peggiore dei casi, all´intera comunità degli utenti. Allo stesso tempo, sono assai scarse le salvaguardie oggi disponibili rispetto alla copia dei dati contenuti nei profili-utente ed al loro utilizzo per costruire profili personali e/o ripubblicare tali dati al di fuori dello specifico servizio di social network(9).
Tuttavia, anche l´utilizzo "normale" dei dati contenuti nei profili-utente può impattare sull´autodeterminazione informativa degli utenti e, ad esempio, incidere gravemente sulle loro possibilità di carriera(10). Un esempio che ha suscitato interesse diffuso riguarda l´abitudine da parte dei dirigenti del personale di singole società di consultare i profili-utente dei candidati all´assunzione e/o dei dipendenti. Secondo quanto riferito da articoli di stampa, già oggi i due

terzi dei dirigenti ammettono di utilizzare i dati ricavati da servizi di social network, ad esempio per verificare e/o completare i curricula dei candidati(11). Altri soggetti che possono trarre profitto da queste fonti di informazione sono le forze dell´ordine e i servizi segreti (anche quelli di Paesi meno democratici con un basso livello di tutela della privacy)(12). Inoltre, alcuni fornitori di servizi di social network forniscono a terzi dati relativi agli utenti tramite interfacce di programmazione di applicativi, e i dati finiscono quindi per essere gestiti dai soggetti terzi in questione(13).

Il Gruppo di lavoro nutre particolari preoccupazioni rispetto al rischio ulteriore di furti d´identità causati dalla disponibilità diffusa di dati personali contenuti nei profili-utente(14) e dall´abuso di tali profili da parte di soggetti terzi non autorizzati.

Utilizzo di un´infrastruttura la cui sicurezza lascia purtroppo molto a desiderare. Si è molto parlato della (non) sicurezza di reti e sistemi informatici, compresi i servizi web. Casi recenti in merito riguardano fornitori di servizi molto conosciuti quali Facebook(15), flickr(16), MySpace(17), Orkut(18), e StudiVZ(19). E´ vero che i fornitori di servizi hanno preso misure atte a potenziare la sicurezza dei loro sistemi, ma molto resta ancora da fare. Allo stesso tempo, è probabile che in futuro emergano nuove falle nella sicurezza di questi sistemi, mentre è assai improbabile che si possa mai conseguire l´obiettivo di una sicurezza totale – vista la complessità delle applicazioni software a qualunque livello dei servizi Internet(20).

I problemi tuttora irrisolti per quanto concerne la sicurezza dei servizi Internet costituiscono un rischio ulteriore connesso all´utilizzo dei servizi di social network e, in certi casi, aumentano il livello complessivo di rischio, ovvero comportano "sfumature" di rischio specifiche di questo tipo di servizi. In un documento recente redatto dalla ENISA (European Network and Information Security Agency) vengono citati, fra l´altro, lo spam, lo scripting fra siti diversi, virus e "vermi", il phishing mirato (spear-phishing) e forme di phishing specifiche dei servizi di social network, l´infiltrazione della rete, l´utilizzo abusivo di profili-utente (profile-squatting) e attacchi reputazionali basati sul furto di identità, forme di persecuzione personale (stalking), il bullismo in rete, e lo spionaggio industriale (ossia, i cosiddetti "social engineering attacks" (strategie basate su interazioni interpersonali finalizzate a carpire informazioni riservate) compiuti attraverso i servizi di social network)(21). Secondo l´ENISA, un rischio ulteriore per la sicurezza è rappresentato "dai fattori di aggregazione legati alle social network"(22).

> *L´introduzione di standard di interoperabilità e interfacce di programmazione applicazioni (API: ad esempio, lo standard "open social" introdotto da Google nel mese di novembre 2007), allo scopo di consentire l´interoperabilità tecnica di servizi di social network tipologicamente diversi, comporta tutta una serie di rischi ulteriori. Si rende infatti possibile una valutazione automatica di tutti i siti di social network che utilizzino lo standard prescelto. Attraverso le API è in pratica l´intera gamma di funzionalità del sistema ad essere passibile di valutazione automatica attraverso l´interfaccia web. Le applicazioni potenzialmente in grado di interferire con la privacy degli utenti (e forse anche con la privacy di soggetti che non sono utenti, ma i cui dati facciano parte di un profilo-utente) comprendono, ad esempio, l´analisi complessiva dei rapporti professionali e privati intrattenuti dal singolo utente, che può senz´altro travalicare i "confini" delle singole social network sulle quali l´utente interagisce volta per volta in ruoli diversi (ad esempio, in un´ottica professionale ovvero più personale e ricreativa); inoltre, l´interoperabilità può favorire in misura ulteriore il riutilizzo da parte di soggetti terzi delle informazioni e delle immagini contenute nei profili-utente, nonché la creazione di profili relativi alle modifiche apportate nel tempo ai singoli profili (con la conseguente disponibilità di informazioni che un utente ha nel frattempo cancellato dal proprio profilo).*

Linee-guida

Alla luce delle considerazioni che precedono, il Gruppo di lavoro formula le seguenti raccomandazioni (in via preliminare) destinate rispettivamente ai soggetti deputati a disciplinare i servizi di social network, ai fornitori di tali servizi ed agli utenti:

Soggetti deputati ad attività di disciplina

Prevedere la possibilità di ricorrere a pseudonimi – ossia, di muoversi nel servizio attraverso uno pseudonimo(23), se già non prevista nell´ambito delle norme di disciplina.

Fare in modo che i fornitori di questi servizi adottino un approccio trasparente nell´indicare le informazioni necessarie per accedere al servizio-base, in modo che gli utenti siano in grado di scegliere a ragion veduta se aderire o meno al singolo servizio, e di opporsi ad eventuali utilizzi secondari (quanto meno rifiutando le opzioni offerte), in particolare per quanto riguarda forme (mirate) di marketing. Si osservi che problemi di ordine specifico si associano al consenso prestato da minori(24).

Introdurre l´obbligo di notifica di eventuali violazioni dei dati relativamente ai servizi di social network. L´unico modo per consentire agli utenti di fare fronte, in particolare, al rischio crescente di furti di identità consiste nel notificare loro ogni violazione della sicurezza dei dati. Così facendo, si potrebbe al contempo ottenere un quadro più preciso dell´effettiva capacità delle imprese di garantire la sicurezza dei dati degli utenti, oltre ad incentivare ulteriormente l´ottimizzazione delle misure di sicurezza adottate.

Ripensare l´attuale assetto normativo con riguardo alla titolarità dei dati personali (in particolare relativi a soggetti terzi) pubblicati sui siti di social network, al fine eventualmente di attribuire ai fornitori di servizi di social network maggiori responsabilità rispetto alle informazioni di natura personale presenti su tali siti.

Potenziare l´integrazione delle tematiche connesse alla privacy nel sistema educativo. Rivelare informazioni personali online è sempre più un fatto normale, soprattutto fra i giovani; pertanto, è necessario che i programmi didattici affrontino tematiche connesse alla privacy ed agli strumenti di autotutela disponibili.

Fornitori di servizi di social network

Per i fornitori di servizi, garantire la sicurezza e la privacy dei dati personali degli utenti è necessariamente questione di sopravvivenza. Se non saranno compiuti rapidi progressi in questo campo, gli utenti potrebbero perdere fiducia (già oggi tale fiducia è assai scossa da casi recentemente verificatisi in cui privacy e sicurezza sono state messe a repentaglio) con un effetto economico negativo paragonabile alla crisi che colpì l´economia digitale verso la fine degli anni ´90.

Garantire la massima trasparenza nell´informare gli utenti rappresenta uno degli elementi più importanti per garantire la correttezza nell´impiego e nel trattamento di dati personali. Si tratta di un requisito fissato nella maggioranza degli strumenti che disciplinano la privacy a livello nazionale, regionale e internazionale; tuttavia, c´è probabilmente bisogno di ripensare alle modalità con cui molti fornitori di servizi oggi informano gli utenti. Oggi, e spesso ciò risponde ai requisiti fissati per legge, l´informativa sulla privacy fa parte delle "condizioni di prestazione del servizio", talora complesse e articolate, rese note dal fornitore del servizio. In alcuni casi viene indicata anche la "privacy policy" seguita da quel determinato servizio. Alcuni fornitori hanno segnalato che, di fatto, solo una bassissima percentuale degli utenti scarica le informazioni in oggetto(25). Anche se l´informativa compare sullo schermo nel momento in cui si aderisce o ci si abbona ad un servizio, ed è accessibile anche in un secondo momento se l´utente lo desidera, è forse più indicato prevedere altre modalità di informazione degli utenti rispetto alle conseguenze potenziali delle attività compiute durante l´utilizzo di un servizio (ad esempio, qualora l´utente modifichi le impostazioni privacy relative, magari, ad un album di immagini), ricorrendo a dispositivi sensibili al contesto (context-sensitive) che permettano di fornire le informazioni volta per volta più opportune.

L´informativa resa all´utente deve comprendere, in modo specifico, informazioni sullo Stato in cui opera il fornitore del servizio, sui diritti riconosciuti agli utenti (accesso, rettifica, cancellazione) rispetto ai loro dati personali, e sulle modalità di finanziamento del servizio stesso. Le informazioni devono essere commisurate alle esigenze specifiche dell´utenza cui

sono indirizzate – soprattutto per quanto riguarda i minori, in modo da consentire decisioni realmente informate.

L´informativa resa all´utente deve prendere in considerazione anche i dati relativi a soggetti terzi. I fornitori dei servizi di social network, oltre ad informare gli utenti sui meccanismi di trattamento dei dati personali di questi ultimi, dovrebbero indicare anche ciò che agli utenti è permesso o non permesso fare con i dati relativi a terzi eventualmente contenuti nei rispettivi profili – ad esempio, in quali casi debbano ottenere il consenso degli interessati prima di pubblicarne i dati, o quali siano le possibili conseguenze se non si rispettano le regole. Particolare importanza rivestono, a tale proposito, le foto che in grandi quantità figurano nei profili-utente e mostrano spesso altre persone (non di rado indicate addirittura con nome e cognome e/o associate ad un link al rispettivo profilo-utente); le prassi vigenti spesso non sono conformi alle norme che disciplinano il diritto all´immagine.

Occorre informare l´utente con chiarezza anche dei rischi comunque esistenti in materia di sicurezza e delle conseguenze derivanti dalla pubblicazione di dati personali in un profilo-utente, nonché della possibilità che soggetti terzi vi abbiano legittimamente accesso (compresi, ad esempio, forze dell´ordine e/o servizi segreti).

Prevedere la possibilità di creare ed utilizzare profili pseudonimizzati, e promuovere il ricorso a tale opzione.

Tenere fede alle promesse fatte agli utenti: Una conditio sine qua non per favorire e conservare la fiducia da parte degli utenti consiste nel fornire informazioni chiare e inequivocabili su ciò che avverrà dei dati degli utenti nelle mani del fornitore del servizio, soprattutto quando si tratti di comunicare i dati a soggetti terzi. Tuttavia, alcuni fornitori di questi servizi sembrano avere un atteggiamento ambiguo rispetto agli impegni presi. L´esempio più chiaro è dato da un´affermazione che ricorre di frequente in questo contesto: "ci impegniamo a non comunicare a chicchessia i suoi dati personali", quando la si applichi alle attività pubblicitarie mirate. Anche se può trattarsi di un´affermazione formalmente corretta, agli occhi del fornitore del servizio, alcuni fornitori in realtà non informano con chiarezza sul fatto che, ad esempio, per far comparire annunci pubblicitari sulla finestra del browser dell´utente può rendersi necessario trasmettere l´indirizzo IP di tale utente ad un altro fornitore di servizi che veicola il contenuto del messaggio pubblicitario – e talora ciò avviene attraverso informazioni che il fornitore del servizio di social network ricava dal profilo dell´utente. E´ vero che le informazioni contenute nel profilo in quanto tali non sono trasmesse al fornitore dei servizi di pubblicità, tuttavia ciò non vale per l´indirizzo IP[(26)] *(a meno che il fornitore di servizi di social network utilizzi, ad esempio, un proxy per nascondere al fornitore di servizi pubblicitari l´indirizzo IP dell´utente). Il problema è che alcuni fornitori di servizi di social network ritengono, erroneamente, che gli indirizzi IP non siano dati personali, mentre in molti Paesi essi in realtà lo sono. Incertezze di questo genere possono risultare fuorvianti per l´utente e minarne la fiducia nel momento in cui l´utente si rende conto di come stiano realmente le cose – e tutto ciò non è né nell´interesse degli utenti, né nell´interesse dei fornitori di servizi. Problemi analoghi riguardano l´utilizzo dei cookies.*

Prevedere impostazioni di default orientate alla privacy è fondamentale per tutelare la privacy degli utenti: è noto che soltanto una minoranza degli utenti che si iscrivono ad un servizio modifica le impostazioni di default, comprese quelle relative alla privacy. In questo caso la scommessa per i fornitori di servizio consiste nel selezionare impostazioni che offrano per default un livello elevato di privacy senza rendere inutilizzabile il servizio stesso; al contempo, la facilità di utilizzo delle funzioni di impostazione è fondamentale per far sì che gli utenti introducano modifiche personali. In ogni caso, per default non dovrebbe essere consentita l´indicizzazione dei profili-utente da parte dei motori di ricerca.

Migliorare il controllo da parte degli utenti sull´utilizzo dei dati contenuti nei loro profili:

a. *All´interno della comunità di utenti*: ad esempio, consentendo limitazioni alla visibilità integrale dei profili e dei dati contenuti in tali profili, nonché limitando la visibilità di tali informazioni nelle funzioni di "ricerca" all´interno della comunità di utenti. L´associazione di specifiche etichette (ad esempio, link a profili-utente in essere, oppure l´apposizione del nome

delle singole persone raffigurate) dovrebbe essere vincolata al previo consenso dell´interessato.

b. *Creare strumenti che consentano agli utenti di controllare l´utilizzo dei dati contenuti nei loro profili da parte di soggetti terzi* – si tratta di un elemento essenziale soprattutto per gestire il rischio di furti di identità. Tuttavia, al momento sono pochi gli strumenti disponibili per controllare le informazioni una volta che siano state pubblicate. L´esperienza dell´industria cinematografica e musicale per quanto concerne le tecnologie di "gestione dei diritti digitali" sembra indicare che anche in futuro le opzioni disponibili saranno piuttosto ridotte. Ciononostante, i fornitori di servizi dovrebbero potenziare le attività di ricerca in questo campo; alcuni approcci già noti e potenzialmente promettenti riguardano la ricerca sul web "semantico" o "policy-aware" [sensibile alle singole politiche][(27)], la cifratura dei profili-utente, la memorizzazione non centralizzata dei profili-utente (ad esempio, presso gli utenti stessi), l´applicazione di filigrane alle immagini fotografiche, l´utilizzo di applicazioni grafiche (anziché testuali) per presentare le informazioni, e l´introduzione di una data di scadenza del profilo-utente, a cura dell´utente stesso[(28)]. Inoltre, i fornitori di questi servizi dovrebbero puntare a scoraggiare gli impieghi secondari, soprattutto delle immagini, mettendo a disposizione degli utenti funzionalità che consentano di trasformare le immagini in dati pseudonimizzati o addirittura anonimi[(29)]. I fornitori dovrebbero adottare misure efficaci anche per impedire che i dati contenuti nei profili-utente siano carpiti da programmi-spider o scaricati/raccolti in massa. Più in particolare, il recupero dei dati relativi agli utenti da parte di motori di ricerca (esterni) dovrebbe essere consentito esclusivamente con il previo consenso espresso ed informato dell´utente interessato.

c. *Consentire agli utenti di controllare gli utilizzi secondari dei dati di traffico e dei dati contenuti nei loro profili* – ad esempio, rispetto l´impiego per scopi di marketing, devono essere previsti come minimo la possibilità di rifiutare il consenso (opt-out) all´uso dei dati personali non sensibili contenuti nel profilo, e l´obbligo di ottenere il consenso espresso (opt-in) per i dati di natura sensibile (opinioni politiche, orientamento sessuale) e per i dati di traffico. In molte delle normative esistenti sono previste disposizioni cogenti in merito all´utilizzo di dati per scopi di marketing, e tali disposizioni devono essere rispettate dai fornitori di servizi di social network. Gli utenti devono essere liberi di scegliere in piena autonomia quali dati, fra quelli contenuti nei rispettivi profili, intendano eventualmente far utilizzare ai fini di un marketing mirato. Inoltre, si potrebbe valutare un´opzione ulteriore, rimessa alla scelta dell´utente: ossia, il pagamento di un importo per finanziare il servizio, anziché l´utilizzo dei dati contenuti nel profilo-utente per scopi di marketing.

d. *Rispettare i diritti riconosciuti agli utenti dalle normative in materia di privacy a livello nazionale, regionale e internazionale*, compreso il diritto degli interessati di ottenere la cancellazione tempestiva dei dati – che in taluni casi può senz´altro comportare la cancellazione dell´intero profilo.

e. *Esaminare le problematiche eventualmente derivanti dalla fusione e/o incorporazione di una società che offra servizi di social network*: Occorre prevedere garanzie per gli utenti rispetto all´osservanza da parte della nuova proprietà degli standard di privacy (e sicurezza) vigenti.

Introdurre adeguati meccanismi per la gestione del contenzioso, ad esempio prevedendo il "congelamento" o il "blocco" di informazioni o immagini oggetto di contestazioni, qualora tali meccanismi non siano già in essere; ciò riguarda gli utenti dei servizi di social network, ma anche i dati personali relativi a soggetti terzi. E´ importante rispondere tempestivamente alle istanze degli interessati. Si possono prevedere misure quali un meccanismo di penalizzazione in caso di condotte abusive relativamente ai dati contenuti nei profili-utenti e ai dati personali di soggetti terzi – ad esempio, escludendo determinati utenti dal sito, se del caso.

Migliorare e mantenere la sicurezza dei sistemi informativi. Ricorrere a buone prassi riconosciute per quanto riguarda la progettazione, la messa a punto e la gestione di applicazioni relative a servizi di social network, compresa la certificazione da parte di soggetti indipendenti.

Elaborare e/o potenziare misure atte a contrastare attività illecite, quali lo spamming ed il furto di identità.

Offrire connessioni cifrate per la gestione dei profili-utente, comprese procedure di log-in sicure.

I fornitori di servizi di social network che operino in più Paesi o livello mondiale devono rispettare gli standard in materia di privacy vigenti nei singoli Paesi in cui sono attivi.

Utenti

Considerazioni conclusive
Il Gruppo di lavoro invita gli organismi per la tutela dei consumatori e della privacy ad adottare le misure opportune onde sensibilizzare i soggetti deputati ad attività di disciplina, i fornitori di servizi, e l´opinione pubblica in genere, ed in particolare i giovani(32), rispetto ai rischi per la loro privacy derivanti dall´utilizzo delle social network, ed alla necessità di un comportamento responsabile nei riguardi dei dati personali propri ed altrui.

Il Gruppo di lavoro intende monitorare con attenzione gli sviluppi futuri relativamente alla tutela della privacy nei servizi di social network, se necessario modificando ed aggiornando le presenti Linee-Guida.

(*) Traduzione non ufficiale

(1) Citazione tratta da Wikipedia http://en.wikipedia.org/wiki/Social_network_service [5 febbraio 2008]

(2) Le linee-guida non prendono in esame chat, blog e siti di ranking.

(3) Un ricercatore tedesco ha di recente individuato, in un campione di servizi di social network fra i più diffusi, circa 120 attributi personali all´interno dei profili utente, quali ad esempio età, indirizzo, film preferiti, libri preferiti, preferenze musicali, ecc. oltre a opinioni politiche e, addirittura, orientamenti sessuali. Si veda „Berliner Morgenpost" 23 gennaio 2008, p. 9: „Mehr Informationen als die Stasi"; http://www.morgenpost.de/content/2008/01/23/wissenschaft/942868.html (in tedesco).

(4) Espressione attribuita a Marc Prensky, conferenziere americano, scrittore, consulente e progettista di giochi educativi e didattici. Si veda p. es. http://www.ascd.org/authors/ed_lead/el200512_prensky.html [5 febbraio 2008]

(5) Già oggi pare che servizi segreti USA (in particolare l´"Open Source Center", presso l´US Director of National Intelligence) utilizzino informazioni tratte dalle cosiddette "fonti perte", fra cui YouTube, ma nche da alcuni "social media" quali MySpace, blog, ecc.; cf. http://www.fas.org/blog/secrecy/2008/02/open_source_intelligence_advan.html

(6) Mentre alcuni fornitori si sono sforzati di creare spazi all´interno dei servizi offerti che diano agli utenti un maggiore controllo sui propri dati personali, altri mettono questi dati (o parte di essi) a disposizione di una platea molto più vasta, e in certi casi dell´intera comunità di utenti – ossia milioni di estranei. "Resta fra noi", vero, ma "noi" può significare anche più di 50 milioni di persone.

(7) Si veda quanto affermato da John Lawford, http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf, p. 35

(8) Si veda ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", ottobre 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

(9) Si osservi che alcuni servizi di social network consentono ai motori di ricerca di navigare nei contenuti relativi agli utenti, e che certi motori di ricerca si sono specializzati da ultimo nell´offrire profili personali ricavati da più fonti. D´altro canto, i fornitori di questi servizi non sembrano ad oggi in grado di incidere sull´attività di spider ("programmi-ragno") che sui rispettivi siti web non rispettino il protocollo "robots.txt".

(10) "26 aprile—Una donna della Pennsilvania afferma di avere avuto distrutta la carriera accademica per colpa dell´amministrazione del suo college, che avrebbe adottato un ingiusto provvedimento nei suoi confronti a causa di una foto su MySpace in cui era ritratta con un cappello da pirata mentre beveva da un bicchiere di plastica. Nel procedimento istituito in base alla legislazione federale (...) si affermava che qualcuno presso la Millersville University l´aveva accusata di favorire l´alcolismo fra i minori dopo avere scoperto quella foto su MySpace (che recava la didascalia "Pirata ubriaco")." Tratto da http://www.thesmokinggun.com/archive/years/2007/0426072pirate1.html [11 febbraio 2008]. Si veda anche The Guardian, 11 gennaio 2008: "Would-be students checked on Facebook"; http://education.guardian.co.uk/universityaccess/story/0,,2238962,00.html

(11) Si veda, ad es., "Employers Use "Facebook" and "MySpace" to Weed Out Applicants"; http://www.wtlv.com/tech/news/news-article.aspx?storyid=64453 [12 febbraio 2008]. L´unico Paese a vietare prassi del genere sembra essere sinora la Finlandia.

(12) Si può pensare che in futuro le autorità responsabili dei controlli sull´immigrazione vi facciano ricorso.

(13) Si veda ad es. "Facebook API Unilaterally Opts Users Into New Services", by Ryan Singel, 25 May 2007, http://blog.wired.com/27bstroke6/2007/05/facebook_api_un.html; cf. anche Chris Soghoian: "Exclusive: The next Facebook privacy scandal", 23 January 2008, http://www.cnet.com/8301-13739_1-9854409-46.html?tag=blog.1 [12 febbraio 2008]

(14) Cf. ad esempio, di recente, gli esperimenti "Natalie" e "frog" condotti dalla Sophos, una società responsabile di sicurezza; cf. "Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Research highlights dangers of irresponsible behaviour on social networking sites", agosto 2007; http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html e "Der Fall ´Natalie´. Online Communities zunehmend IT-Sicherheits-Risiko. Experten warnen vor massivem Anstieg von Datendiebstahl und -missbrauch auf Social Network Websites", 21 gennaio 2008 (in tedesco).

(15) Cf. "Secret Crush Facebook App Installing Adware, Security Firm Charges", Wired del 3 gennaio 2008, .ht http://blog.wired.com/27bstroke6/2008/01/secret-crush-faml

(16) Cf. "Phantom Photos: My photos have been replaced with those of another"; http://flickr.com/help/forum/33657/

(17) Cf. ad es. "MySpace XSS QuickTime Worm", dicembre 2006; http://www.websense.com/securitylabs/alerts/alert.php?AlertID=708

(18) Cf. [marzo 2008]

(19) Cf. ad es. „Datenleck beim StudiVZ? [Update]"; http://www.heise.de/newsticker/meldung/81373/ (in tedesco).

(20) Inoltre, la rapida crescita della mole di informazioni memorizzate in formato elettronico di anno in anno è considerata di per sé come un rischio in termini di sicurezza. Durante l´ultima RSA Europe Security Conference tenutasi nel 2007 a Londra, il presidente della RSA, Art Coviello, aveva affermato che nel solo 2006 erano stati generati a livello mondiale 176 esabyte di dati, e che a suo parere una mole simile di informazioni era ingestibile e non poteva essere messa in sicurezza secondo meccanismi efficaci – si veda la rivista tedesca specializzata in informatica "iX", dicembre 2007, p. 22 "Trübe Aussichten: Große Datenmengen verhindern Datensicherheit" (in tedesco); http://www.heise.de/kiosk/archiv/ix/2007/12/022/

(21) Cf. ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", ottobre 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

(22) Cf. ENISA Position Paper No.1, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, p. 12

(23) In questo ambito, "utilizzare uno pseudonimo" significa il diritto di muoversi in un servizio di social network attraverso uno pseudonimo, senza dover rivelare la "vera" identità ad altri utenti del servizio o al pubblico in genere, se questo è ciò che l´utente desidera. A seconda dei casi, ciò può comportare la comunicazione della vera identità al fornitore del servizio all´atto della registrazione.

(24) Cf. Working Paper "Childrens´ Privacy On Line: The Role of Parental Consent", adottato in occasione della 31ma riunione, Auckland (Nuova Zelanda), 26/27 marzo 2002; http://www.datenschutz-berlin.de/attachments/205/child_en.pdf

(25) Di recente, un rappresentante di Facebook ha affermato, in occasione di una conferenza OCSE, che la percentuale degli utenti che visitano le pagine contenenti privacy policy probabilmente non supera lo 0.25%; cf. http://www.stenotran.com/oecd/2007-10-03-Session4b.pdf p. 33f. [6 febbraio 2008].

(26) A seconda delle circostanze, il fornitore dei contenuti pubblicitari può addirittura essere in grado di ricostruire parte o la totalità delle informazioni contenute nel profilo attraverso la tipologia dei messaggi pubblicitari mirati destinati al singolo utente.

(27) Cf. ad es. Daniel J. Weitzner, Jim Hendler, Tim Berners-Lee, Dan Connolly: "Creating a Policy-Aware Web: Discretionary, Rule-based Access for the World Wide Web". Di prossima pubblicazione in: Web and Information Security, E. Ferrari and B. Thuraisingham (eds), Idea Group Inc., Hershey, PA; http://www.w3.org/2004/09/Policy-Aware-Web-acl.pdf, e Sören Preibusch, Bettina Hoser, Seda Gürses, and Bettina Berendt: Ubiquitous social networks – opportunities and challenges for privacy-aware user modelling; http://vasarely.wiwi.hu-berlin.de/DM.UM07/Proceedings/05-Preibusch.pdf [12 febbraio 2008].

(28) Cf. ad es. The Royal Academy of Engineering: Dilemmas of Privacy and Surveillance. Challenges of Technological Change. Marzo 2007, par. 7.2.1, p. 40

(29) Cf. ENISA Position Paper No.1: "Security Issues and Recommendations for Online Social Networks", ottobre 2007, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf, p.23

(30) Cf. ad es. la brochure "when online gets out of line" pubblicata congiuntamente da facebook e dall´Information and Privacy Commissioner of Ontario, Canada, http://www.ipc.on.ca/images/Resources/up-facebook_ipc.pdf,; US Federal Trade Commission: "Social Networking Sites: A Parent´s Guide", http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.shtm e "Social Networking Sites: Safety Tips for Tweens and Teens" http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.shtm

(31) Cf. ad es. le impostazioni proposte come modello da Sophos per facebook; http://www.sophos.com/security/best-practice/facebook.html

(32) Cf. ad es. la campagna „dubestemmer" lanciata dall´Autorità norvegese di protezione dati; http://www.dubestemmer.no/english.php, il progetto "DADUS" dell´Autorità portoghese di protezione dati; http://dadus.cnpd.pt, e le iniziative di cui alla nota 30, supra.