Il controllo nei social network

Avv. Monica Gobbato

E-Privacy 2009

www.monicagobbato.it

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

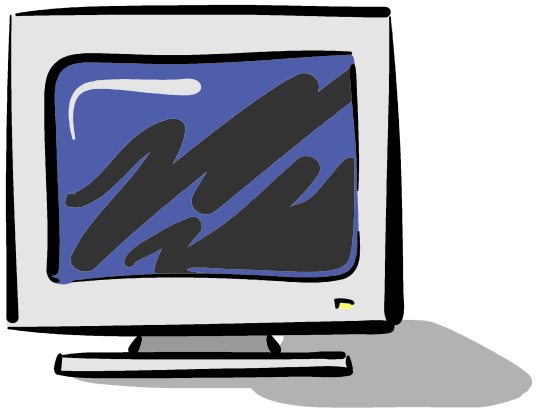
INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS

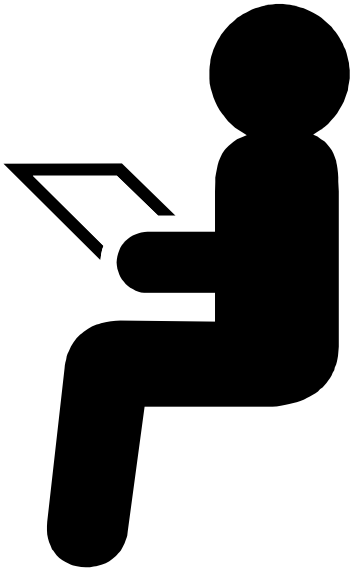
Rapporto

"Un servizio di *social network* (rete sociale) consiste nella creazione e nel controllo di reti sociali online destinate a comunità di soggetti che condividono

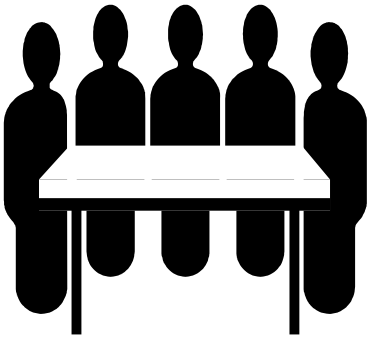
determinati interessi e attività, ovvero intendono esplorare gli interessi e le attività di altri soggetti, necessariamente attraverso l'impiego di applicazioni software. Si tratta in maggioranza di servizi basati sull'utilizzo del web;

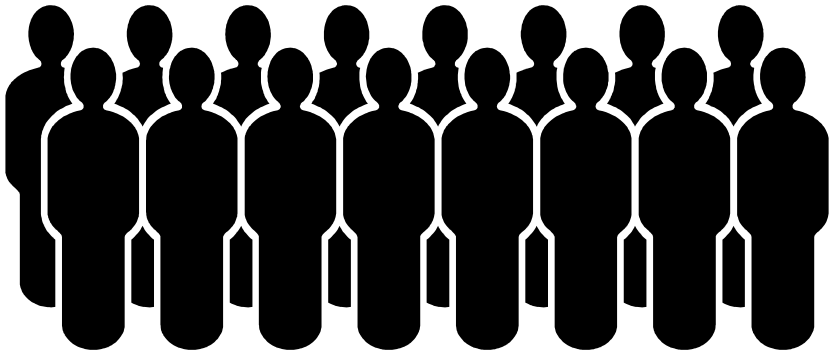
numerose sono le modalità di interazione fra gli utenti [...](1). Più specificamente, molti siti offrono strumenti per interagire con altri abbonati (sulla base di profili personali generati autonomamente)"(2).

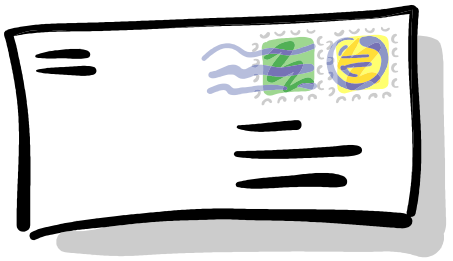




Un ricercatore tedesco ha di recente individuato, in un campione di servizi di social network fra i più diffusi, circa 120 attributi personali all'interno dei profili utente, quali ad esempio età, indirizzo, film preferiti, libri preferiti, preferenze musicali, ecc. oltre a opinioni politiche e, addirittura, orientamenti sessuali.







- **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.**

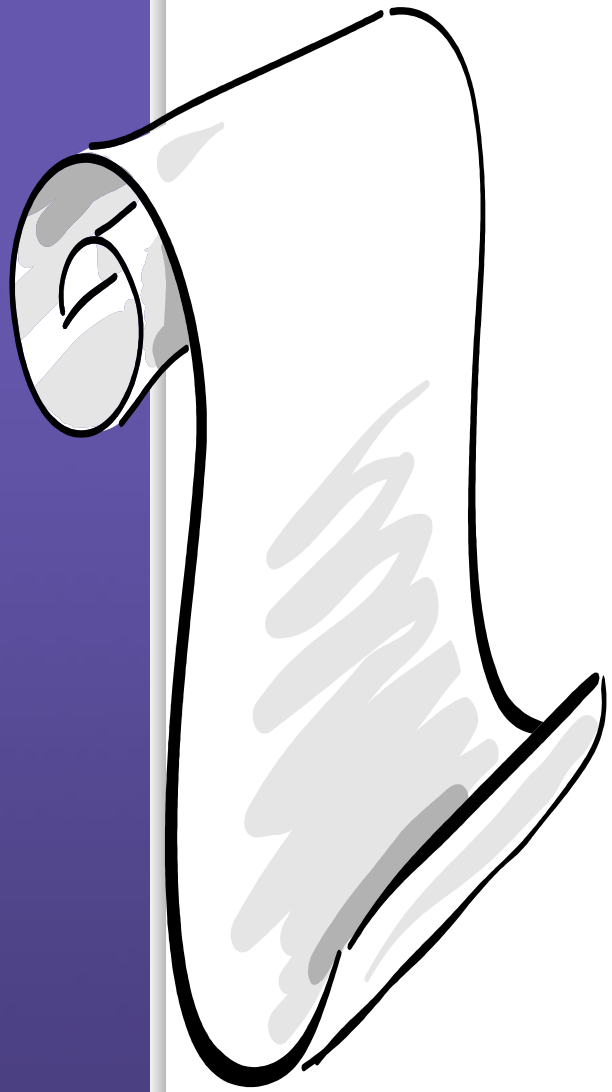
- Mentre le norme "tradizionali" in materia di privacy vertono sulla definizione di regole che tutelino i cittadini dal trattamento sleale o sproporzionato dei loro dati personali da parte dei soggetti pubblici (compresi polizia e servizi segreti) e delle imprese, vi **sono pochissime norme che disciplinino 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 pubblic_{he.}

Nuova Generazione di Utenti

- **(4)** Espressione attribuita a Marc Prensky, conferenziere americano, scrittore, consulente e progettista di giochi educativi didattici.

- **... 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

… nuove opportunità di comunicazione e scambio di informazioni di ogni genere, in tempo reale



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**.

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.

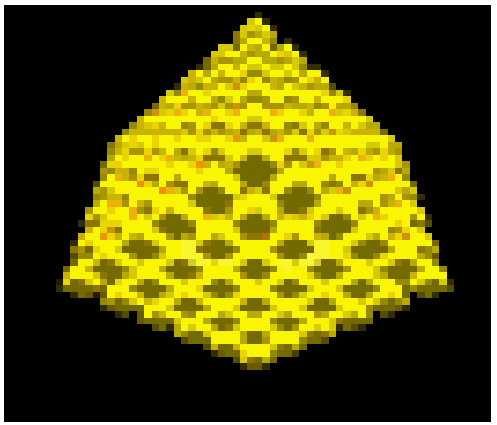
- ***L'idea ingannevole di "comunità".*** Molti fornitori affermano di trasferire le strutture comunicative dal mondo "reale" al cyberspazio. Un'affermazione frequente è che non ci sarebbero problemi, per esempio, a pubblicare dati (personali) su queste piattaforme, perché è come se si condividessero 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 s. n. i quali **hanno gli strumenti tecnici per registrare ogni singolo passo dell'utente sul loro sito** e, 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 il trattamento di dati relativi agli utenti, trattandosi dell'unico cespite patrimoniale dei fornitori di servizi di s. n.. I siti non sono 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.

- ***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. 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. 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 i dati personali contenuti nei profili 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 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 articoli di stampa, già oggi i due terzi dei dirigenti ammettono di utilizzare i dati ricavati da servizi di s. n. ad esempio per verificare e/o completare i curricula dei candidati(11). Altri soggetti che possono trarre profitto da queste informazioni sono le forze dell'ordine e i servizi segreti (anche quelli di Paesi meno democratici con un basso livello di tutela della privacy)(12).

Ulteriori Rischi

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). Secondo l'ENISA, un rischio ulteriore per la sicurezza è rappresentato "dai fattori di aggregazione legati alle social network"(22).

si possono identificare le persone anche in base a dati non riferibili a persone ma oggetti Esempio: controllo della posizione dei taxi per ottimizzare il servizio

Linee-guida

Alla luce delle considerazioni svolte il Gruppo di lavoro formula le seguenti raccomandazioni 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 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

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.

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

Risoluzione sulla tutela della privacy nei servizi di social network

Raccomandazioni

Reputazione On Line

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

Educazione

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 uno 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.

La privacy degli altri

Gli utenti devono rispettare la privacy altrui. Occorre particolare attenzione se si pubblicano

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:

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.

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. 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

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 privacy; solo una minoranza degli utenti che aderiscono ad un determinato servizio si preoccupa di modificare tali impostazioni. Le impostazioni in oggetto devono essere particolarmente restrittive se il servizio di social network è destinato o rivolto a minori.

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

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.

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.

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.

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.

Furto d'identità

La sentenza n. 46674/2007 Corte di Cassazione

Sostituzione di persona attraverso una e-mail

La quinta sezione della Cassazione conferma la condanna, ex articolo 494 del Codice Penale, nei confronti di chi utilizzava le generalità di un'altra persona per accedere a servizi e comunicare con altri utenti.

La norma in questione recita:

"***Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria persona all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno***"

Cassazione V Sezione Penale n. 46674 del 14 dicembre 2007

SVOLGIMENTO

Con l'impugnata sentenza è stata confermata la dichiarazione di colpevolezza di A.M.A. in ordine al reato p. e p. dagli artt. 81, 494 c.p., contestatogli "perché, al fine di procurarsi un vantaggio e di recare un danno ad A.T., creava un account di posta elettronica, ********@libero.it., apparentemente intestato a costei, e successivamente, utilizzandolo, allacciava rapporti con utenti della rete internet al nome della A.T., e così induceva in errore sia il gestore del sito sia gli utenti, attribuendosi il falso nome della A.T.".

Ricorre per cassazione il difensore deducendo violazione di legge per l'erronea applicazione dell'art. 494 c.p. e per la mancata applicazione dell'art. 129 c.p.p.

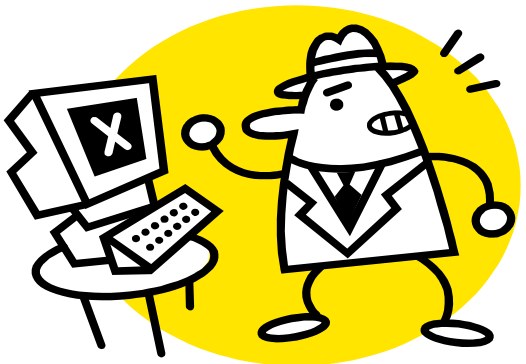
TESI DEL RICORRENTE

Il ricorrente disserta in ordine alla possibilità per chiunque di attivare un “account” di posta elettronica recante un nominativo diverso dal proprio, anche di fantasia.
Ciò è vero, pacificamente.
Ma deve ritenersi che il punto del processo che ne occupa sia tutt’altro.

Secondo la Corte...

Tali doglianze non possono essere condivise.

Oggetto della tutela penale, in relazione al delitto preveduto nell'art. 494 c.p.,**è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali.** E siccome si tratta di inganni che possono superare la ristretta cerchia d'un determinato destinatario, così il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome.



Secondo la Corte...

il **soggetto indotto in errore non è tanto l'ente fornitore del servizio di posta elettronica, quanto piuttosto gli utenti della rete**, i quali, ritenendo di interloquire con una determinata persona (la A.T.), in realtà inconsapevolmente si sono trovati ad avere a che fare con una persona diversa.

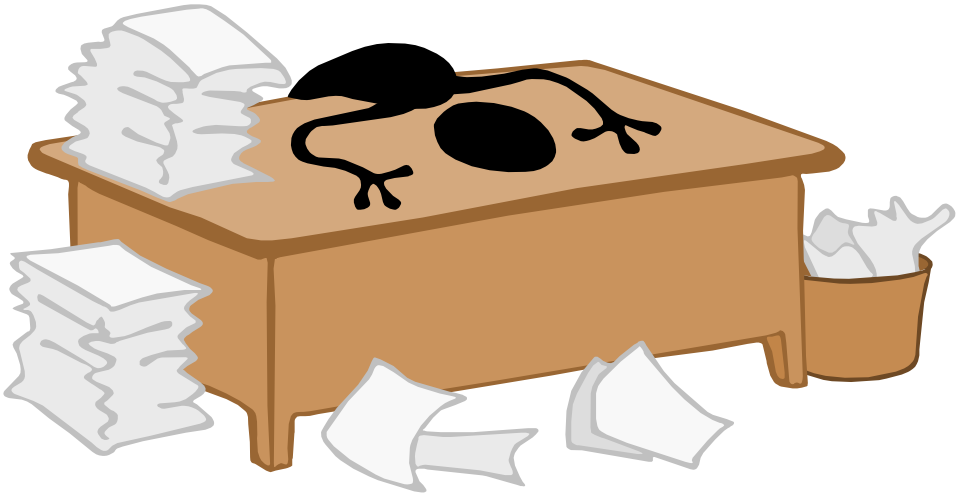
l’imputazione ex art. 494 c.p.p. debitamente menziona...

pure il fine di recare - con la sostituzione di persona - un danno al soggetto leso: danno poi in effetti, in tutta evidenza concretizzato, nella specie **al reato di diffamazione,** nitidamente delinea nella subdola inclusione della persona offesa in una corrispondenza idonea a ledere l’immagine o la dignità (sottolinea la sentenza impugnata che la A.T., a seguito dell’iniziativa assunta dall’imputato, “si ricevette telefonate da uomini che le chiedevano incontri a scopo sessuale”).

Monica Gobbato

Home	Profilo	Colleghi	Posta
		Altre aree	

	Info	Progetti in atto	Link	Area Riservata
Bacheca			Siti utili	
	Descrizione delle attività e del profilo			



Grazie...

Avv. Monica Gobbato
gobbatomonica@tiscali.it