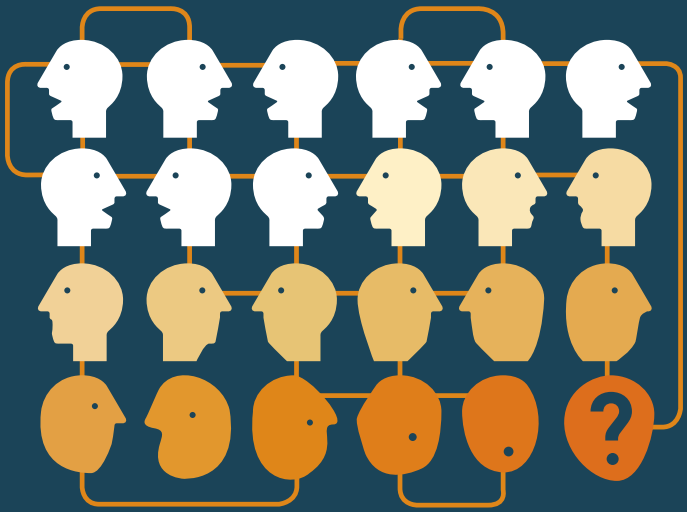
# SOCIAL NETWORK:
## ATTENZIONE AGLI EFFETTI COLLATERALI



Il vademecum è stato realizzato prima dell'applicazione del Regolamento UE 679/2016, avvenuta in data 25 maggio 2018, circostanza di cui occorre tener conto nella consultazione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

**FACEBOOK & CO**

**AVVISO AI NAVIGANTI**

**TI SEI MAI CHIESTO?**

**CONSIGLI**
**PER UN USO CONSAPEVOLE**
**DEI SOCIAL NETWORK**

**IL GERGO DELLA RETE**

# SOCIAL NETWORK:
## ATTENZIONE AGLI EFFETTI COLLATERALI

Facebook, MySpace & Co. È vivo il dibattito tra coloro che esaltano le rivoluzionarie possibilità di comunicazione offerte dai social network e coloro che ne vedono solo i pericoli per la vita privata e i diritti dei naviganti.

Il Garante per la privacy ha deciso di mettere a punto una breve guida per aiutare chi intende entrare in un social network o chi ne fa già parte a usare in modo consapevole uno strumento così nuovo. Non un manuale esaustivo, ma un agile vademecum sia per persone alle prime armi, sia per utenti più esperti.

L'obiettivo è anche quello di offrire spunti di riflessione e, soprattutto, consigli per tutelare, anche nel "mondo virtuale", uno dei beni più preziosi che abbiamo: la nostra identità, i nostri dati personali.

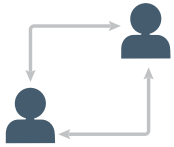
# FACEBOOK & CO

## I SOCIAL NETWORK

I social network (Facebook, MySpace e altri) sono "piazze virtuali", cioè dei luoghi in cui via Internet ci si ritrova portando con sé e *condividendo* con altri fotografie, filmati, pensieri, indirizzi di amici e tanto altro.
I social network sono lo strumento di condivisione per eccellenza e rappresentano straordinarie forme di comunicazione, anche se comportano dei rischi per la sfera personale degli individui coinvolti.

I primi social network sono nati in ambito universitario, tra colleghi che non si volevano "perdere di vista", che desideravano "fare squadra" una volta entrati nel mondo del lavoro. Facebook, per citare uno dei più famosi, agli inizi era esattamente la traduzione virtuale del "libro delle fotografie" della scuola, dell'annuario. Una bacheca telematica dove ritrovare i colleghi di corso e scambiare con loro informazioni. Gli ultimi sviluppi spingono i social network a integrarsi sempre più con i telefoni cellulari, trasformando i messaggi che pubblichiamo on-line in una sorta di sms multiplo che giunge istantaneamente a tutti i nostri amici.

Gli strumenti predisposti dalle reti sociali ci permettono di seguire i familiari che vivono in un'altra città. Espandono la nostra possibilità di comunicare, anche in ambito politico e sociale trasformandoci in agenti attivi di campagne a favore di quello in cui crediamo. Possono facilitare lo scambio di conoscenze tra colleghi, e tra colleghi e impresa.



I social network sono strumenti che danno l'impressione di uno spazio personale, o di piccola comunità. Si tratta però di un falso senso di intimità che può spingere gli utenti a esporre troppo la propria vita privata, a rivelare informazioni strettamente personali, provocando "effetti collaterali", anche a distanza di anni, che non devono essere sottovalutati.

### ALCUNI DEI SOCIAL NETWORK PIÙ DIFFUSI NEL MONDO

Facebook, MySpace, Hi5, Flickr, Skyrock, Friendster, Tagged, LiveJournal, Orkut, Fotolog, Bebo.com, LinkedIn, Badoo.Com, Multiply, Imeem, Ning, Last.fm, Twitter, MyYearbook, Vkontakte, aSmallWorld, Windows Live, Xiaonei.

### IL GARANTE E LE TUTELE SU INTERNET

Il Garante per la protezione dei dati personali segue con attenzione gli sviluppi delle forme di comunicazione su Internet ed è impegnato a livello europeo e internazionale per definire regole e comportamenti che tutelino gli utenti e le libertà individuali.
La forma di tutela più efficace è comunque sempre l'autotutela, cioè la gestione attenta dei propri dati personali.

# AVVISO AI NAVIGANTI

**PER SEMPRE... O QUASI**
Quando inserisci i tuoi dati personali su un sito di social network, ne perdi il controllo. I dati possono essere registrati da tutti i tuoi contatti e dai componenti dei gruppi cui hai aderito, rielaborati, diffusi, anche a distanza di anni. A volte, accettando di entrare in un social network, concedi all'impresa che gestisce il servizio la licenza di usare senza limiti di tempo il materiale che inserisci on-line... le tue foto, le tue chat, i tuoi scritti, i tuoi pensieri.

**DISATTIVAZIONE O CANCELLAZIONE?**
Se decidi di uscire da un sito di social network spesso ti è permesso solo di "disattivare" il tuo profilo, non di "cancellarlo". I dati, i materiali che hai messo on-line, potrebbero essere comunque conservati nei *server*, negli archivi informatici dell'azienda che offre il servizio. Leggi bene cosa prevedono le *condizioni d'uso* e le garanzie di privacy offerte nel contratto che accetti quando ti iscrivi.

**LE LEGGI APPLICATE**
La maggior parte dei siti di social network ha sede all'estero, e così i loro server. In caso di disputa legale o di problemi insorti per violazione della privacy, non sempre si è tutelati dalle leggi italiane ed europee.

**CHI PUÒ FARE COSA**
Il miglior difensore della tua privacy sei tu. Rifletti bene prima di inserire on-line dati che non vuoi vengano diffusi o che possano essere usati a tuo danno. Segnala al Garante le eventuali violazioni affinché possa intervenire a tua tutela.

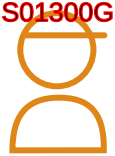
**LA PRIVACY DEGLI ALTRI**
Quando metti on-line la foto di un tuo amico o di un familiare, quando lo *tagghi* (inserisci, ad esempio, il suo nome e cognome su quella foto), domandati se stai violando la sua privacy. Nel dubbio chiedi il consenso.

**LA LOGICA ECONOMICA**
Le aziende che gestiscono i social network generalmente si finanziano vendendo pubblicità mirate. Il valore di queste imprese è strettamente legato anche alla loro capacità di analizzare in dettaglio il profilo, le abitudini e gli interessi dei propri utenti, per poi rivendere le informazioni a chi ne ha bisogno.

**NON SONO IO!**
Attenzione ai falsi *profili*.
Basta la foto, il nome e qualche informazione sulla vita di una persona per impadronirsi on-line della sua *identità*. Sono già molti i casi di attori, politici, persone pubbliche, ma anche di gente comune, che hanno trovato su social network e blog la propria identità gestita da altri.

**E IL CONTO IN BANCA?**
Attenti alle informazioni che rendete disponibili on-line. La data e il luogo di nascita bastano per ricavare il vostro codice fiscale. Altre informazioni potrebbero aiutare un malintenzionato a risalire al vostro conto in banca o addirittura al vostro nome utente e alla password.

# TI SEI MAI CHIESTO?



**SEI UN RAGAZZO/A :**

- Se sapessi che il vicino di casa o il tuo professore potrebbero leggere quello che hai inserito on-line, scriveresti le stesse cose e nella stessa forma?
- Sei sicuro che le foto e le informazioni che pubblichi ti piaceranno anche tra qualche anno?
- Prima di *caricare/postare* la "foto ridicola" di un amico, ti sei chiesto se a te farebbe piacere trovarti nella stessa situazione?
- I membri dei gruppi ai quali sei iscritto possono leggere le tue informazioni personali?
- Sei sicuro che mostreresti "quella" foto anche al tuo nuovo ragazzo/a?

**SEI UN GENITORE:**

- Hai spiegato a tuo figlio che non deve toccare il fornello acceso, lo hai educato ad attraversare la strada, a "non prendere caramelle dagli sconosciuti"... ma gli hai insegnato a riconoscere i segnali di pericolo in rete?
- Gli hai insegnato a difendersi dalle aggressioni dei potenziali provocatori, degli adescatori on-line? A non raccontare a tutti, anche a sconosciuti, la sua vita privata e quella degli amici?
- Hai mai provato a navigare insieme a tuo figlio? Gli hai chiesto di mostrarti come si usa Internet? A quali gruppi è iscritto?
- Gli hai mai chiesto se è stato vittima di *cyberbullismo*?

**CERCHI LAVORO:**

- Sai che le società di selezione del personale cercano informazioni sui candidati utilizzando i principali motori di ricerca on-line?
- Le foto che hai pubblicato sui social network, e i *post* che hai inserito potranno danneggiarti nella ricerca del tuo prossimo lavoro?
- Il curriculum che hai spedito all'azienda corrisponde con quello che hai messo su Internet?
- Quello che racconti della tua vita nelle tue "chiacchiere on-line" è coerente con le tue aspirazioni professionali?

**SEI UN UTENTE "ESPERTO":**

- Hai verificato come sono impostati i livelli di privacy della tua identità?
- Hai violato il diritto alla riservatezza di qualcuno pubblicando "quel" materiale?
- Hai commesso un reato mostrando quelle foto a tutti, scrivendo quei *post*?
- Hai verificato chi detiene la "licenza d'uso", le "royalty" e la proprietà intellettuale della documentazione, delle immagini o dei video che hai inserito on-line?

**SEI UN PROFESSIONISTA:**

- Il gruppo di persone abilitate a interagire con la tua *identità* corrisponde al target professionale che ti sei prefissato di raggiungere?
- I gruppi ai quali sei iscritto sui social network possono avere effetti negativi sul tuo lavoro?
- Se vieni contestato on-line da un componente iscritto alla tua rete di social network, sei preparato a reagire in maniera appropriata?
- Hai valutato se stai *condividendo* informazioni con qualcuno che può danneggiarti?
- Sai che numerosi servizi di *chat* – inclusi quelli offerti dai siti di social network – permettono di registrare e conservare il contenuto della conversazione avvenuta con gli altri utenti?

# CONSIGLI PER UN USO CONSAPEVOLE DEI SOCIAL NETWORK

**AUTOGOVERNO**

Pensa bene prima di pubblicare tuoi dati personali (soprattutto nome, indirizzo, numero di telefono) in un *profilo*-utente, o di accettare con disinvoltura le proposte di amicizia.

**PENSARCI PRIMA**

Ricorda che immagini e informazioni possono riemergere, complici i motori di ricerca, a distanza di anni.

**RISPETTARE GLI ALTRI**

Astieniti dal pubblicare informazioni personali e foto relative ad altri senza il loro consenso. Potresti rischiare anche sanzioni penali.

**CAMBIARE LOGIN E PASSWORD**

Usa login e password diversi da quelli utilizzati su altri siti web, sulla posta elettronica e per la gestione del conto corrente bancario on-line.

### PSEUDONIMI

Se possibile crea pseudonimi differenti in ciascuna rete cui partecipi.
Non mettere la data di nascita o altre informazioni personali nel *nickname*.

### ESSERE INFORMATI

Informati su chi gestisce il servizio e quali garanzie offre rispetto al trattamento dei dati personali. Ricorda che hai diritto di sapere come vengono utilizzati i tuoi dati: cerca sotto privacy o *privacy policy*.

### LIVELLI DI PRIVACY

Utilizza impostazioni orientate alla privacy, limitando al massimo la disponibilità di informazioni, soprattutto per quanto riguarda la reperibilità dei dati da parte dei motori di ricerca. Controlla come sono impostati i livelli di privacy del tuo profilo: chi ti può contattare, chi può leggere quello che scrivi, chi può inserire commenti alle tue pagine, che diritti hanno gli utenti dei gruppi ai quali appartieni.

### ATTENZIONE ALL'IDENTITÀ

Non sempre parli, *chatti* e *condividi* informazioni con chi credi tu. Chi appare come bambino potrebbe essere un adulto e viceversa. Sempre più spesso vengono create false identità (sia di personaggi famosi, sia di persone comuni) per semplice gioco, per dispetto o per carpire informazioni riservate. Basta la tua foto e qualche informazione sulla tua vita... e il prossimo "clonato" potresti essere tu.

### SPAM / PUBBLICITÀ INDESIDERATA

Controlla come vengono utilizzati i tuoi dati personali da parte del fornitore del servizio. Se non desideri ricevere pubblicità, ricordati di rifiutare il consenso all'utilizzo dei dati per attività mirate di pubblicità, promozioni e marketing.

### CONTRATTO E CONDIZIONI D'USO

Leggi bene il contratto e le *condizioni d'uso* che accetti quando ti iscrivi a un social network. Controlla anche le modifiche che vengono introdotte unilateralmente dall'azienda. Verifica di poter recedere facilmente dal servizio, e di poter cancellare tutte le informazioni che hai pubblicato sulla tua identità.

# IL GERGO DELLA RETE

**ALIAS / FAKE**
Falsa identità assunta su Internet (ad esempio su siti di social network). L'utente può scegliere un nome di fantasia, uno pseudonimo, o appropriarsi dei dati di una persona realmente esistente. A volte il termine fake viene utilizzato per segnalare una notizia falsa.

**BANNARE / BANDIRE**
L'atto che l'amministratore di un sito o di un servizio on-line (chat, social network, gruppo di discussione...) effettua per vietare l'accesso a un certo utente. In genere si viene bannati/cancellati quando non si rispettano le regole di comportamento definite all'interno del sito.

**CARICARE / UPLODARE / UPLOADARE**
Inserire un documento di qualunque tipo (audio, video, testo, immagine) on-line, anche sulla bacheca del proprio profilo di social network.

**CHATTARE**
Sistema di messaggistica testuale istantanea. Termine mutuato dalla parola inglese "chat", letteralmente, "chiacchierata". Il dialogo on-line può essere limitato a due persone, o coinvolgere un gruppo più ampio di utenti.

**CONDIVIDERE**
Permettere ad altri utenti, amici/sconosciuti, di accedere al materiale (testi, audio, video, immagini) che sono presenti sul nostro computer o che abbiamo caricato on-line.

**CONDIZIONI D'USO / USER AGREEMENT / TERMS OF USE**
Le regole contrattuali che vengono accettate dall'utente quando accede a un servizio. È sempre bene stamparsele e leggerle con attenzione quando si decide di accettarle. Possono essere modificate in corso d'opera dall'azienda.

**PRIVACY POLICY / TUTELA DELLA PRIVACY / INFORMATIVA**
Pagina esplicativa predisposta dal gestore del servizio – a volte un semplice estratto delle Condizioni d'uso del sito - contenente informazioni su come saranno utilizzati i dati personali inseriti dall'utente sul sito di social network, su chi potrà usare tali dati e quali possibilità si hanno di opporsi al trattamento. (Per una definizione completa del termine "informativa" e una spiegazione dei diritti e dei doveri in tema di privacy, consultare il sito Internet www.garanteprivacy.it)

**SCARICARE /DOWNLODARE / DOWNLOADARE**
Salvare sul proprio computer o su una memoria esterna (dischetto, chiave usb, hard disk esterno...) documenti presenti su Internet. Ad esempio: le fotografie o i video trovati su siti quali Facebook o su Youtube.

**SERVER**
Generalmente, si tratta di un computer connesso alla rete utilizzato per offrire un servizio (ad esempio per la gestione di un motore di ricerca o di un sito di social network). Sono denominati "client" i computer (come quello di casa) che gli utenti utilizzano per collegarsi al server e ottenere il servizio.

**TAG**
Marcatore, "etichetta virtuale", parola chiave associata a un contenuto digitale (immagine, articolo, video).

**TAGGARE**
Attribuire una "etichetta virtuale" (tag) a un file o a una parte di file (testo, audio, video, immagine). Più spesso, sui social network, si dice che "sei stato taggato" quando qualcuno ha attribuito il tuo nome/cognome a un volto presente in una foto messa on-line. Di conseguenza, se qualcuno cerca il tuo nome, appare la foto indicata.

**CYBERBULLISMO**
Indica atti di molestia/bullismo posti in essere utilizzando strumenti elettronici. Spesso è realizzato caricando video o foto offensive su Internet, oppure violando l'identità digitale di una persona su un sito di social network.
Si tratta di un fenomeno sempre più diffuso tra i minorenni.

**IDENTITÀ / PROFILO / ACCOUNT**
Insieme dei dati personali e dei contenuti caricati su un sito Internet o, più specificamente, su un social network. Può indicare anche solo il nome-utente che viene utilizzato per identificarsi e per accedere a un servizio on-line (posta elettronica, servizio di social network, chat, blog...).

**LOGGARE / AUTENTICARSI**
Accedere a un sito o servizio on-line, facendosi identificare con il proprio nome-utente (login, user name) e password (parola chiave).

**NICKNAME**
Pseudonimo.

**POKARE / MANDARE UN POKE**
È l'equivalente digitale di uno squillo telefonico fatto a un amico per attirarne l'attenzione. In origine, su Facebook, con un "poke" (cenno di richiamo) si chiedeva a uno sconosciuto il permesso di accedere temporaneamente al suo profilo per decidere se inserirlo nella propria rete di amici.

**POSTARE**
Pubblicare un messaggio (post) – non necessariamente di solo testo - all'interno di un newsgroup, di un forum, di una qualunque bacheca on-line.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771
fax 06 696773785

Per informazioni:
Ufficio per le relazioni
con il pubblico
Lunedì - Venerdì ore 10.00 - 13.00
e-mail: urp@garanteprivacy.it

A cura del Servizio relazioni
con i mezzi di informazione
del Garante per la protezione
dei dati personali

Vertigo Design

www.garanteprivacy.it