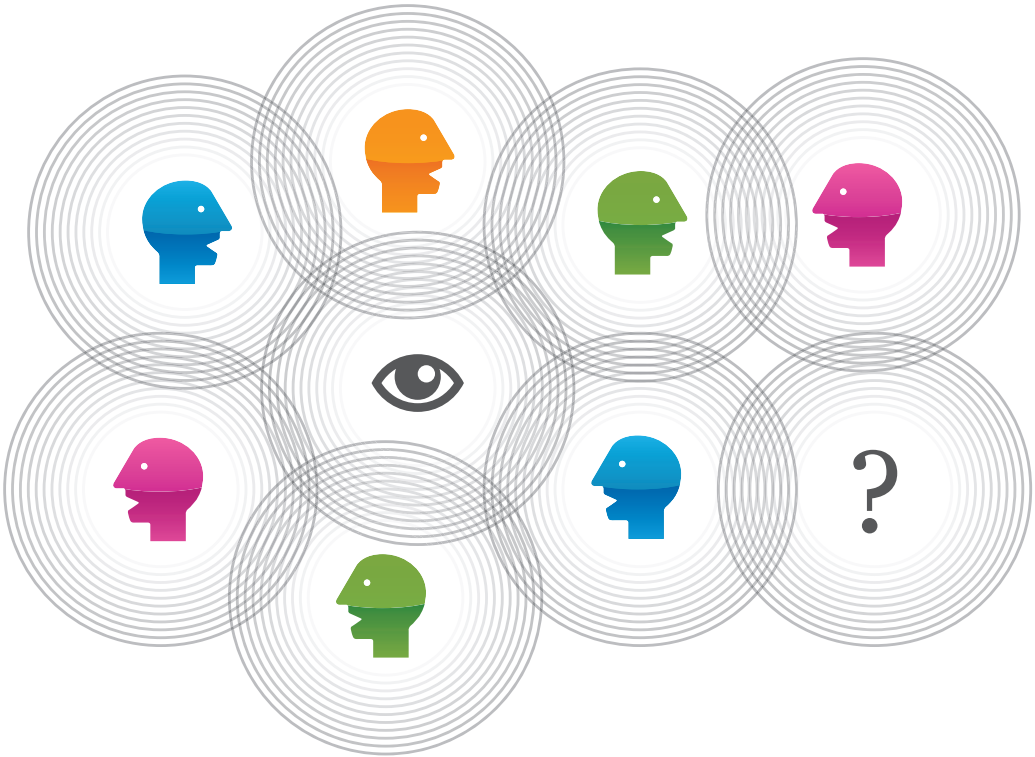
SOCIAL PRIVACY

COME TUTELARSI NELL'ERA DEI SOCIAL NETWORK



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

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

FACEBOOK & CO

AVVISI AI NAVIGANTI

TI SEI MAI CHIESTO?

10 CONSIGLI
PER NON RIMANERE
INTRAPPOLATI

IL GERGO DELLA RETE

PREMESSA:
DALLA VITA DIGITALE A QUELLA REALE

Il mondo delle reti sociali (da Facebook a Twitter, da Linkedin a Instagram) è in cambiamento incessante e il Garante per la protezione dei dati personali ne segue con attenzione gli sviluppi allo scopo di tutelare con efficacia giovani e adulti.

I social network offrono vantaggi significativi e immediati: semplificano i contatti, rendono possibili scambi di informazioni con un numero enorme di persone. Queste comunità on-line, però, amplificano i rischi legati a un utilizzo improprio o fraudolento dei dati personali degli utenti, esponendoli a danni alla reputazione, a furti di identità, a veri e propri abusi.

Non esistono più, infatti, barriere tra la vita digitale e quella reale: quello che succede on-line sempre più spesso ha impatto fuori da Internet, nella vita di tutti i giorni e nei rapporti con gli altri.

Proprio con l'obiettivo di aumentare la consapevolezza degli utenti e offrire loro ulteriori spunti di riflessione e strumenti di tutela, il Garante ha deciso di aggiungere nuovi contenuti alla guida ai social network pubblicata nel 2009, mantenendone però la struttura agile che ne ha favorito in questi anni la diffusione e il facile utilizzo.

FACEBOOK & CO

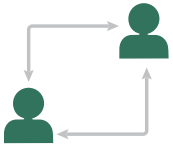
I SOCIAL NETWORK

I social network (a volte definiti social media per enfatizzare il loro impatto non solo come reti sociali ma come veri e propri media auto-organizzati) sono "piazze virtuali", cioè dei luoghi in cui via Internet ci si ritrova condividendo con altri fotografie, filmati, pensieri, indirizzi, 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" e 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 dell'annuario, ovvero del "libro delle fotografie" della scuola. Una bacheca telematica dove ritrovare i colleghi di corso e scambiare con loro informazioni. Le più recenti evoluzioni della tecnologia consentono ai social network di 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.

Ai tradizionali social network si sono aggiunte numerose piattaforme di messaggistica sociale istantanea (come WhatsApp), la cui crescita è andata di pari passo con la rapidissima diffusione di smartphone e di altri strumenti (dai tablet ai phablet, alle cosiddette tecnologie indossabili come occhiali e orologi "intelligenti") che consentono la connessione alla rete in mobilità.



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 e professionale, a rivelare informazioni confidenziali, orientamenti politici, scelte sessuali, fede religiosa o condizioni di salute, provocando gravi "effetti collaterali", anche a distanza di anni, che non devono essere sottovalutati. Tra l'altro, l'idea di impunità trasmessa dalla possibilità di utilizzare messaggi che si "autodistruggono" o di nascondersi dietro forme di anonimato può favorire in rete atteggiamenti aggressivi o violenti, in particolare verso le persone più giovani e indifese.

ALCUNI DEI SOCIAL NETWORK PIÙ DIFFUSI NEL MONDO

Facebook, Google Plus+, VKontakte, Qzone, WhatsApp, LinkedIn, Badoo, Twitter, LINE, WeChat, SinaWeibo, Orkut, Snapchat, Vine, Tencent QQ, Instagram, MySpace, Ask.fm, Tumblr.

IL GARANTE E LA PRIVACY SU INTERNET

La dignità della persona e il diritto alla riservatezza non perdono il loro valore su Internet. La tutela dei dati personali nel mondo interconnesso, per quanto più difficile, è pur sempre possibile, anche grazie alla collaborazione tra i Garanti della privacy, non soltanto europei, ma anche di altri Paesi. L'Autorità italiana interviene direttamente in caso di violazioni di propria competenza. Ma è anche costantemente impegnata per rafforzare gli strumenti a difesa degli utenti e per aumentare la loro consapevolezza sui loro diritti e doveri on-line.

AVVISI AI NAVIGANTI

VITA DIGITALE – VITA REALE
Non esiste più una separazione tra la vita "on-line" e quella "off-line". Quello che scrivi e le immagini che pubblichi sui social network hanno quasi sempre un riflesso diretto sulla tua vita di tutti i giorni, e nei rapporti con amici, familiari, compagni di classe, colleghi di lavoro. Ed è bene ricordare che l'effetto può non essere necessariamente immediato, ma ritardato nel tempo.

IL RICORDO DEL FAR WEST
Il web è spesso raccontato come un luogo senza regole dove ogni utente può dire o fare quello che vuole. In realtà, le stesse regole di civile convivenza, così come le norme che tutelano, ad esempio, dalla diffamazione, dalla violazione della tua dignità, valgono nella vita reale come sui social network, in chat o sui blog. Non esistono zone franche dalle leggi e dal buon senso.

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 al fornitore del servizio la licenza di usare senza limiti di tempo il materiale che inserisci on-line... le tue foto, le tue chat, i tuoi scritti, le tue opinioni.

IL MITO DELL'ANONIMATO
Non è poi così difficile risalire all'identità di coloro che pubblicano testi, immagini, video su Internet con l'intento di danneggiare l'immagine o la reputazione di un'altra persona. L'anonimato in rete può essere usato per necessità, ma mai per commettere reati: in questo caso le autorità competenti hanno molti strumenti per intervenire e scoprire il "colpevole".

LA PRIVACY E IL RISPETTO 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 chiedigli il consenso. Non lasciarti trascinare dagli hater, dai troll, nel gioco perverso dei gruppi "contro qualcuno": la prossima volta potresti essere tu la vittima.

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

GIOCARE E FARSI MALE
Molti giovani, ma non soltanto loro, pensano che l'adozione di alcuni piccoli stratagemmi, come l'invio di messaggi che si "autodistruggono" dopo la lettura, possa metterli al riparo dai rischi di un uso inappropriato del materiale che viene così condiviso. Questa falsa sicurezza può spingerti a scambiare, senza pensarci troppo, messaggi sessualmente espliciti (sexting), insulti gratuiti o semplicemente inopportuni. Tutto quello che è condiviso, però, può sempre essere in qualche maniera salvato e riutilizzato. Se stai giocando, attento a non farti male.

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

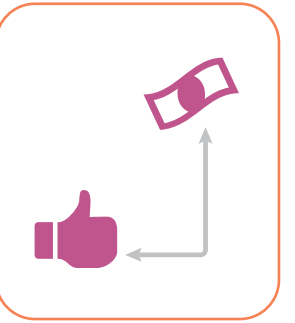
DISATTIVAZIONE O CANCELLAZIONE?
Se decidi di uscire da un social network spesso ti è permesso solo di "disattivare" il tuo profilo, non di "cancellarlo". I dati, i materiali che hai messo on-line, potrebbero essere comunque conservati nei server, negli archivi informatici dell'azienda che offre il servizio. 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 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. Se desideri essere più sicuro sul rispetto dei tuoi diritti, sappi che le società che ti offrono i loro servizi da sedi dislocate in uno dei Paesi dell'Unione Europea devono sempre rispettare la normativa comunitaria e in essi è presente un'autorità di protezione dati (Data Protection Authority) che potrà intervenire, anche tramite il Garante, nel caso subissi violazioni alla tua privacy.

CHI PUÒ FARE COSA
Rifletti bene prima di inserire on-line dati che non vuoi vengano diffusi o che possano essere usati a tuo danno. Segnala al Garante della privacy e alle altre autorità competenti le eventuali violazioni affinché possano intervenire a tua tutela. Ma ricorda: il miglior difensore della tua privacy sei innanzitutto tu.

LA LOGICA ECONOMICA:
NIENTE È GRATIS

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 degli utenti, le abitudini e i loro hobby, ma anche le condizioni di salute e l'orientamento politico o sessuale, le reti di contatti, per poi rivendere le informazioni a chi se ne servirà per promuovere offerte commerciali specifiche o per sostenere campagne di vario genere.
Le informazioni raccolte su di te sono infatti usate per monitorare e prevedere i tuoi acquisti, le tue scelte, i tuoi comportamenti.
E ricorda: anche nel web, dietro l'offerta di un servizio "gratuito", si nasconde lo sfruttamento per molteplici scopi dei tuoi dati.



CI SONO AMICI E AMICI
Nelle amicizie esistono differenti livelli di relazione a seconda che ci si rapporti con amici stretti o semplici conoscenti, compagni di classe o professori, partner commerciali o datori di lavoro. Sui social network spesso poniamo tutti sullo stesso piano, rischiando di scrivere o mostrare la cosa sbagliata alla persona sbagliata. Impara a distinguere chi aggiungi alla tua rete di "amici" in base all'uso che ne fai. Se il social network a cui sei iscritto te lo consente, decidi quali tipi di informazioni possono essere consultate dai differenti tipi di amici.

LA REPUTAZIONE DELLE IMPRESE
Anche le società che offrono servizi on-line e di social network hanno una reputazione da mantenere di fronte all'opinione pubblica. Gran parte del loro valore di mercato e del numero di iscritti dipende anche dalla loro "immagine". Se una società adotta comportamenti scorretti nei confronti degli utenti o non risponde con celerità a richieste di aiuto – ad esempio contro il cyberbullismo e la diffamazione – parlane con gli altri utenti e segnalalo alle autorità competenti.

TI SEI MAI CHIESTO?

SEI UN RAGAZZO/A:

- Se sapessi che il vicino di casa o il tuo professore possono accedere al tuo profilo e al tuo diario 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 informazioni riservate che posti sul tuo profilo?
- Sei sicuro che mostreresti "quella" foto con il tuo ex anche al tuo nuovo ragazzo/a?
- Vuoi veramente far sapere a chiunque dove ti trovi (si chiama geolocalizzazione) e chi stai incontrando in ogni momento della giornata?
- Prima di inviare, anche per gioco, un video sexy al tuo nuovo compagno, hai considerato che potrebbe essere condiviso con i suoi amici o con degli sconosciuti?

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 della rete?
- Gli hai insegnato a difendersi dalle aggressioni di potenziali provocatori o molestatori on-line? A non raccontare a tutti, anche a sconosciuti, particolari della sua vita privata e di quella degli amici?
- Hai mai provato a navigare insieme a tuo figlio? Gli hai chiesto di mostrarti come si usa Internet e le reti sociali alle quali è iscritto? Se vedi tua figlia turbata, le chiedi come è andata la giornata con i suoi gruppi sui social network?
- Provi mai a farti spiegare dai tuoi figli quali sono gli argomenti di discussione più interessanti sui social network in quel momento? Ti informi se i tuoi figli hanno conosciuto nuovi amici in chat?
- Hai cercato di capire se sono stati vittime di cyberbullismo o stalking o se fanno sexting?
- Sai come funzionano le "app" sociali e di messaggistica istantanea che i tuoi figli hanno caricato sullo smartphone?
- Conosci i rispettivi vantaggi e gli svantaggi che una persona ha nel collegarsi a un social network con la propria identità riconoscibile o in forma anonima? Ne hai discusso con i tuoi figli?

CERCHI LAVORO:

- Sai che le società di selezione del personale cercano informazioni sui candidati utilizzando i principali motori di ricerca on-line o accedendo direttamente ai profili pubblicati sui social network?
- Ti sei chiesto se le foto che hai pubblicato sui social network e i post che hai inserito potranno danneggiarti nella ricerca del tuo prossimo lavoro?
- Le informazioni contenute nel curriculum che hai spedito all'azienda corrispondono a quelle che hai pubblicato su Internet, magari sul tuo profilo?
- Quello che racconti della tua vita nelle tue "chiacchiere on-line" è coerente con le tue aspirazioni professionali?
- Lo sai che a volte basta cliccare un "mi piace" sui social network per essere "analizzati ed etichettati" in base alle proprie opinioni politiche, sessuali o religiose, con eventuali ripercussioni anche sul contesto lavorativo?

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?
- Prima di installare sul tuo smartphone o sul tuo tablet una nuova "app", hai verificato a quali dati personali accede il programma? E per quale motivo?

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 sul 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?
- Quando offri un servizio ai tuoi clienti, chiedi di essere retribuito per il tuo lavoro. Ti sei mai domandato come paghi i servizi "gratuiti" e le "app" che utilizzi su Internet?

10 CONSIGLI PER NON RIMANERE INTRAPPOLATI

1

PENSARCI BENE, PENSARCI PRIMA

Pensa bene prima di pubblicare i tuoi dati personali (soprattutto nome, indirizzo, numero di telefono) in un profilo-utente, o di accettare con disinvoltura le proposte di amicizia. Ricorda che immagini e informazioni che posti in rete possono riemergere, complici i motori di ricerca, a distanza di anni. Fai attenzione a quello che fai on-line e alle informazioni che condividi (in particolare se riguardano la tua salute o altri aspetti ancora più intimi) anche in forum o chat, perché potrebbe avere "effetti collaterali" sulla tua vita reale.

2

NON SENTIRTI TROPPO SICURO

Prendi opportune precauzioni per tutelare la tua riservatezza, ma non illuderti di essere sempre al sicuro. Le foto e i video che scambi privatamente, magari di contenuto esplicito, possono essere sempre copiati e inoltrati ad altre persone "fuori dal giro dei tuoi amici". Non esistono, tra l'altro, messaggi che si autodistruggono con assoluta certezza.

3

RISPETTA GLI ALTRI

Astieniti dal pubblicare informazioni personali e foto relative ad altri (magari "taggandone" i volti) senza il loro consenso. Sui social network e nella messaggistica istantanea uno scherzo o una semplice ripicca può facilmente degenerare in un grave abuso, facendoti rischiare anche sanzioni penali.

4

SERRA LA PORTA DELLA TUA RETE E DEL TUO SMARTPHONE

Aggiorna l'antivirus del tuo smartphone. 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. Fai attenzione, inoltre, quando clicchi su uno dei tanti indirizzi internet abbreviati (ad esempio url tipo t.co, bit.ly oppure goo.gl) pubblicati sui social network, e verifica che non ti conducano a siti fasulli usati per rubarti i dati o per farti scaricare programmi con virus. Se possibile crea pseudonimi differenti in ciascuna rete cui partecipi. Non mettere la data di nascita (in particolare se sei minorenne) o altre informazioni personali nel nickname: così potrai rendere più difficile "tracciarti" o molestarti.

5

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.

6

OCCHIO AI CAVILLI

Informati su chi gestisce il social network 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".
Accertati di poter recedere facilmente dal servizio e di poter cancellare (eventualmente anche di poter salvare e trasferire) tutte le informazioni che hai pubblicato sulla tua identità.
Leggi bene il contratto e le condizioni d'uso che accetti quando ti iscrivi a un social network. Controlla con attenzione anche le frequenti modifiche che vengono introdotte unilateralmente dal fornitore del servizio: capita spesso che i social network comunichino di aver cambiato i livelli di privacy che tu hai scelto per la tua identità solo alla fine di una lunga nota.

7

ANONIMATO, MA NON PER OFFENDERE

Se lo ritieni opportuno, pubblica messaggi sotto pseudonimo o in forma anonima per tutelare la tua identità, non per offendere o violare quella degli altri. Difendi la libertà di parola, non di insulto. Ricordati che in caso di violazioni non è poi così difficile risalire agli autori di messaggi anonimi postati su Internet.

8

FATTI TROVARE SOLO DAGLI AMICI

Se non vuoi far sapere a tutti dove sei stato o dove ti trovi, ricordati di disattivare le funzioni di geolocalizzazione presenti sulle "app" dei social network, così come sullo smartphone e sugli altri strumenti che utilizzi per collegarti a Internet.

9

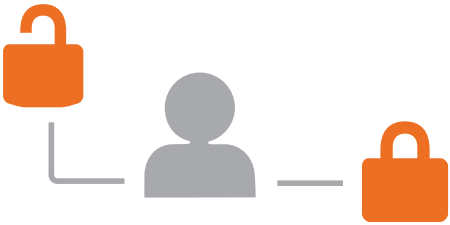
SEGNALA L'ABUSO E CHIEDI AIUTO

Se noti comportamenti anomali e fastidiosi su un social network, se vedi che un tuo amico è insultato e messo sotto pressione da individui o gruppi, non aspettare e segnala subito la situazione critica al gestore del servizio affinché possa intervenire immediatamente. A tale scopo, alcuni social network rendono accessibile agli utenti, sulle pagine del proprio sito, un'apposita funzione (una sorta di pulsante "panic button") per chiedere l'intervento del gestore contro eventuali abusi o per chiedere la cancellazione di testi e immagini inappropriate.
In caso di violazioni, segnala subito il problema al Garante e alle altre autorità competenti. Se sei tu la vittima di commenti odiosi a sfondo sessuale, di cyberbullismo o di sexting, se stanno violando la tua privacy, non aspettare che la situazione degeneri ulteriormente e chiedi aiuto alle persone a te care e alle autorità compenti.

10

PIÙ SOCIAL PRIVACY, MENO APP E SPAM

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. Limita al massimo la disponibilità di informazioni, soprattutto per quanto riguarda la reperibilità dei dati da parte dei motori di ricerca.
Controlla quali diritti di accesso concedi alle App che installi sul tuo smartphone o sul tuo tablet affinché non possano utilizzare i tuoi dati personali (contatti, telefonate, foto...) senza il tuo consenso. Se non desideri ricevere pubblicità, ricordati che puoi rifiutare il consenso all'utilizzo dei dati per attività mirate di pubblicità, promozioni e marketing.



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.

APP
Un software che si installa su smartphone, tablet o altri dispositivi portatili. Può offrire funzionalità di ogni tipo, come l'accesso ai social network, le previsioni del tempo, il consumo di calorie, i videogiochi, le novità musicali. Il termine deriva dalla contrazione del termine "applicazione".

ASKARE
Descrive una pratica molto diffusa negli adolescenti iscritti al social network Ask.fm, ovvero quello di postare una domanda personale, quasi sempre in forma anonima, sulla bacheca di uno degli utenti registrati. Questo meccanismo può facilitare atteggiamenti aggressivi o di vero e proprio cyberbullismo.

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
Termine mutuato dalla parola inglese "chat", letteralmente, una "chiacchierata". Il dialogo on-line, attraverso un sistema di messaggistica istantanea, 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 stamparle e leggerle con attenzione quando si decide di accettarle. Possono essere modificate in corso d'opera dall'azienda.

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...).

GEOLOCALIZZAZIONE
Identificazione della posizione geografica di un utente. Tra le tante modalità con cui viene rilevata si ricordano: il segnale gps dello strumento che si sta utilizzando oppure la triangolazione delle reti wi-fi rilevate dallo strumento con cui l'utente si collega in rete.

HASHTAG
Il termine deriva dall'unione dei due termini inglesi hash (cancelletto) e tag (etichetta). Il carattere "#" viene anteposto dagli utenti di alcuni social network alle parole chiave dei propri messaggi. I messaggi così indicizzati possono essere raggruppati e ricercati in base all'argomento segnalato.

HATER
Letteralmente "chi odia". Il termine viene spesso utilizzato per indicare chi pubblica, spesso coperto dall'anonimato, messaggi offensivi o carichi di rabbia.

LOGGARE / AUTENTICARSI
Accedere a un sito o a un servizio on-line, facendosi identificare con il proprio nome-utente (login, username) 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.

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 (chiave usb, hard disk esterno...) documenti presenti su Internet. Ad esempio, le fotografie o i video trovati su siti quali Facebook o Youtube.

SELFIE
Indicano gli autoscatti o, comunque, le fotografie di se stessi. La pubblicazione di gallerie di "selfie" rappresenta una tendenza abbastanza comune in rete.

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.

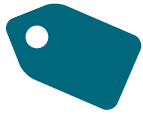
SEXTING
Consiste nell'invio di messaggi provocanti o sessualmente espliciti (eventualmente con foto o video). Il termine sexting deriva dall'unione di due parole inglesi: sex (sesso) e texting (inviare messaggi testuali). Lo scambio di messaggi a contenuto erotico direttamente tramite cellulare o attraverso altri strumenti connessi in rete (come social network e posta elettronica) è molto diffuso tra gli adolescenti.

SNAPCHATTARE
"Fare uno snapchat" o snapchattare indica lo scambio di messaggi che si autodistruggono sul social network Snapchat.

SPAM
Pubblicità e offerte commerciali indesiderate. Sui social network si diffondono spesso forme elaborate di "social spam".

STALKING
Il termine stalking viene utilizzato con varie accezioni ma generalmente indica l'adozione di atti persecutori ripetuti (ad esempio tramite sms, telefonate o forme di pedinamento) nei confronti di qualcuno. In rete, tali attività moleste e intrusioni nella vita privata possono essere condotte con e-mail o altri tipi di "messaggi istantanei" oppure scambi indesiderati sui social network.

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.

TROLLING
Definisce il comportamento di chi agisce on-line come un "troll", provocando, insultando, aggredendo, pubblicando commenti negativi nei confronti di altri utenti della comunità virtuale.

TWEET
La traduzione inglese del termine "cinguettio". Identifica un breve messaggio inviato sul social network Twitter.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121 - 00186 Roma
tel. 06 696771 – fax 06 696773785
www.garanteprivacy.it

Antonello Soro, Presidente
Augusta Iannini, Vice Presidente
Giovanna Bianchi Clerici, Componente
Licia Califano, Componente

Giuseppe Busia, Segretario generale

Per informazioni presso l'Autorità:
Ufficio per le relazioni con il pubblico
lunedì - venerdì ore 10.00 - 13.00
tel. 06 696772917
e-mail: urp@gpdp.it
pec: urp@pec.gpdp.it

**A cura del Servizio relazioni
con i mezzi di informazione**

Vertigo Design - Stampa: IAG Mengarelli - Maggio 2014