EDUCARE ALLA RETE

L'alfabeto della nuova cittadinanza nella società digitale

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

EDUCARE ALLA RETE

L’alfabeto della nuova cittadinanza nella società digitale

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Indice

Educare alla Rete

Lo sviluppo impetuoso delle tecnologie digitali ha trasformato con incredibile velocità e con effetti difficilmente prevedibili l'organizzazione sociale del nostro tempo.

Questi effetti non sono interamente percepiti.

Internet da strumento di comunicazione si è trasformato in presupposto dell'agire individuale, principale piattaforma su cui costruire relazioni interpersonali, lavoro ed erogazione di servizi, commerci e contenuti: è diventato l'ambiente in cui nasce la cultura e si forma un modo di abitare il mondo e di organizzarlo.

Occorre prendere consapevolezza che questo ambiente non è un luogo separato, una realtà parallela ma piuttosto lo spazio in cui si dispiega una parte sempre più importante della vita reale.

Reale e virtuale non possono più essere declinati come due mondi distinti dove ciascuno è libero di assumere una diversa identità a seconda della circostanza, ma rappresentano ormai territori integrati da una costante e sempre più pervasiva "connettività".

Questo processo ha subito una straordinaria accelerazione per effetto di molteplici fattori: dalla proliferazione delle connessioni mobili alla progressiva integrazione dei diversi strumenti di comunicazione, alla forza innovativa delle applicazioni tecnologiche che diventano sempre più piccole e indossabili quasi a costituire appendici del nostro corpo, capaci di aumentarne e potenziarne le funzioni. Se un'applicazione per smartphone calcola il percorso più veloce per andare a casa e un'altra monitora funzioni vitali del nostro corpo come, ad esempio, la frequenza cardiaca, o il consumo calorico o piuttosto il livello di attenzione nella guida dell'automobile; se la profilazione comportamentale personalizzata non si basa sulla registrazione dei testi raccolti in Rete ma utilizza sensori capaci di cogliere altre dimensioni delle nostre attività, captare ed elaborare elementi non linguistici ma espressivi di emozioni, allora si pongono problemi davvero nuovi per i quali non abbiamo risposte adeguate.

La tecnologia diventa pervasiva e si trasforma in una seconda pelle che condiziona ineluttabilmente gli stili di vita.

Siamo immersi nel digitale e sempre di più conosceremo noi stessi, il mondo e gli altri attraverso la tecnologia e sarebbe illusoria la pretesa di arrestare questa evoluzione con un semplicistico invito a "scollegarsi" o "disconnettersi".

La quotidianità si è già modificata ed ha trovato nelle tecnologie digitali strumenti per esprimere nuove esigenze alle quali è impossibile ed irrealistico rinunciare.

La materialità delle cose si è ridotta: la maggior parte delle attività - dalle amicizie, allo scambio di semplici pensieri, agli spostamenti - si è smaterializzata dando luogo ad una produzione massiccia di dati digitali che circolano, in modo incessante, attraverso la Rete e, soprattutto, attraverso i dispositivi mobili che implacabilmente e continuamente li raccolgono e trasmettono.

La rivoluzione digitale che trasforma in dati parti sempre più rilevanti delle nostre vite private propone problemi nuovi per le nostre libertà.

Nello spazio digitale si possono violare le nostre persone, si possono negare i diritti, si possono manipolare o perfino rubare informazioni che riguardano strettamente aspetti fondamentali della nostra esistenza, che coincidono con la nostra vita.

La tentazione più insidiosa per tutti noi consiste nella rassegnazione a considerare che tutto ciò che si trasforma in byte sia altro rispetto alla nostra fisicità, qualcosa di lontano rispetto alla nostra vita quotidiana.

La sfida più grande che dobbiamo affrontare è quella di riuscire ad accompagnare la società in un processo di elaborazione delle misure, della cultura e della sensibilità necessarie per far fronte ai nuovi problemi posti dallo sviluppo tecnologico.

Se, infatti, un'esperienza millenaria ci ha trasmesso ed insegnato la necessità di proteggere e tutelare i beni materiali, dobbiamo riconoscere che siamo ancora inesperti e privi di adeguate capacità di fronte ai lati oscuri dello spazio digitale.

Gli hacker che, attraverso virus o codici, aprono la serratura di banche dati o siti protetti sono ladri esattamente come coloro che utilizzano un grimaldello per aprire una porta blindata. Il furto dell'identità digitale o di un profilo Facebook reca alla vittima un danno anche maggiore rispetto alla sottrazione del portafoglio o di un'agenda personale. Ed ancora: forme di monitoraggio continuo in Rete non sono semplicemente un fastidio e una inammissibile invadenza, ma armi puntate contro di noi: i dati digitali tracciati, controllati, archiviati possono al momento opportuno essere utilizzati per danneggiarci.

Occorre trovare nuove forme per tutelare la persona nella sua unicità tra vita fisica e vita digitale.

Così come nutriamo una legittima aspettativa di integrità e sicurezza quando ci muoviamo nello spazio fisico, dove esistono regole, leggi, consuetudini, mezzi di tutela per prevenire situazioni di pericolo e rimuovere ostacoli al libero dispiegamento della nostra personalità, allo stesso modo deve essere presidiato lo spazio digitale, nel quale si svolge una parte rilevante delle nostre vite e che, dunque, non può essere affidato all'arbitrio di chi quello spazio conquista.

Proteggere il flusso di dati con i quali comunichiamo, e dunque, "viviamo" significa proteggere noi stessi e le nostre esistenze.

La rivoluzione digitale attacca e scompiglia le tradizionali categorie giuridiche. Ma non possiamo permettere che gli eventi ci soverchino e che inerzia e situazioni di fatto favoriscano l'oblio del diritto.

Dobbiamo sfuggire due tentazioni estreme e opposte: da una parte quella di una inutile e stupida tecnofobia, la fuga dall'innovazione, l'idea apocalittica che attribuisce alla Rete la colpa di tutti i mali della modernità e, dall'altra, la rinuncia rassegnata a contrastare le distorsioni del sistema, a ricercare una qualche regolazione dei processi globali che presiedono alla comunicazione elettronica e più in generale a vivere responsabilmente il nostro tempo.

La questione è complessa: il bisogno di regolare la Rete per coniugare libertà e responsabilità nel più grande spazio pubblico del nostro tempo è tema che appassiona e divide le opinioni pubbliche in ogni parte del pianeta.

E la risposta va trovata, auspicabilmente in una dimensione sovranazionale. Per questo è di estrema importanza la Risoluzione approvata nel novembre 2013 dall'ONU proprio sul tema della "Privacy nell'era digitale" con la quale si invitano gli Stati membri ad operare per prevenire le violazioni del "diritto umano alla privacy" e si sottolinea la necessità che nel mondo on-line i diritti debbano godere della identica tutela offerta loro nel mondo reale. Nella stessa prospettiva, anche le Autorità garanti per la protezione dei dati del mondo, riunite nella 35ma Conferenza internazionale di Varsavia, hanno adottato una specifica Risoluzione proprio sulla promozione dell'educazione digitale. L'obiettivo è quello di impegnare i Governi affinché venga assicurata particolare protezione ai minori e garantita una formazione permanente degli educatori sui rischi della tecnologia, che deve sempre promuovere il rispetto degli utenti.

Un'adeguata protezione dei dati si pone dunque come garanzia ineludibile per scongiurare il pericolo che le nuove tecnologie, indispensabili nel semplificare l'attività dei singoli individui, agevolare l'interscambio di informazioni, migliorare la vita di relazione, si traducano in strumenti perversi e potenzialmente lesivi.

Ed invero, il valore racchiuso nelle regole e nei comportamenti in cui si sostanzia il diritto alla protezione dei dati assolve ad un ruolo di fondamentale rilievo nella ricerca del bilanciamento tra uomo e tecnica, tra società in continua evoluzione e capacità di adattamento dell'individuo.

Essere sicuri che i dati siano protetti costituisce una condizione essenziale affinché si continui a garantire ed assicurare l'effettivo godimento delle libertà e dei diritti tradizionalmente riconosciuti, difesi e tutelati nel mondo off line.

Parti della nostra vita sono disseminate e conservate nelle grandi banche dati, dove la nostra identità è sezionata, scomposta e spesso ricomposta come un mosaico di tessere diversamente raccolte.

In una società che compra e vende informazioni e fa diventare merce la stessa persona alla quale si riferiscono i dati, la tutela della privacy diventa sempre più una questione di libertà.

Si tratta di valori fondamentali che devono in primo luogo essere trasmessi ai giovani - i cosiddetti

“nativi digitali” - che più di altri possiedono le capacità per accedere e sfruttare in modo sempre più dinamico le opportunità offerte dalla società digitale. Usano computer, smartphone e tablet come pratiche abituali per comunicare con i coetanei, accedere alle informazioni, autoesporsi aggiornando continuamente i propri status, postando commenti, pubblicando foto o video ed immettendo on-line una quantità impressionante di dati personali che rivelano pensieri, emozioni, abitudini, amicizie.

Nella maggior parte dei casi, i ragazzi che conoscono alla perfezione i meccanismi e la forza del web e delle innovazioni, non sanno ancora valutare appieno le conseguenze delle proprie azioni: e questo li rende particolarmente vulnerabili. Bisogna convincere i ragazzi, che si muovono a volte in modo compulsivo tra il mondo digitale e quello reale, che la vita vera è ovunque: in Rete e fuori dalla Rete.

L'illusorio anonimato che Internet sembra garantire (attraverso ad esempio l’utilizzo di nickname o profili falsi) spesso permette di ledere e calpestare senza rispetto i dati sensibili, rubare identità, demolire psicologicamente, con comportamenti aggressivi, i compagni. Molestie, minacce, diffamazione, gravi fattispecie sanzionate dal codice penale, non perdono certo di significato se realizzate nel web.

Tutto ciò che facciamo in Rete diventa il contenuto delle nostre vite, delle nostre biografie, che ne saranno condizionate per sempre, soprattutto a causa della stessa dimensione indeterminata ed indefinita della Rete.

Occorre invertire la rotta ed evitare che i giovani siano sfruttati e percepiti soltanto come consumatori passivi di tecnologia, incoraggiandoli a comprendere i principi fondamentali e, soprattutto, i rischi (sempre più invisibili) che si corrono.

Così come non lasciamo cartelli per avvertire i ladri dell’assenza da casa, allo stesso modo dovremmo imparare ad evitare di lasciare minuziosi dettagli sui nostri spostamenti sui social network; così come ci hanno insegnato a non dare confidenza agli sconosciuti, egualmente dovremmo evitare di inserire i dettagli delle nostre vite, soprattutto se intimi, su Internet.

La scuola potrebbe svolgere un ruolo di primo piano, prevedendo specifici progetti educativi

nell'ambito dei programmi scolastici che insegnino ai giovani il modo di confrontarsi costruttivamente con le nuove forme espressive offerte dalla Rete, al fine di promuovere una gestione consapevole di tutti gli aspetti della propria vita che vengono consegnati al mondo on-line.

Dal canto loro, gli educatori ed i formatori devono essere aiutati a colmare il deficit di conoscenza dei nuovi fenomeni e strumenti comunicativi.

Anche per questo motivo tutti gli attori istituzionali - il Governo, il Parlamento ma anche il servizio pubblico radiotelevisivo - sono chiamati ad una nuova missione.

Tutti dobbiamo misurarci con le sfide di una complessa fase di transizione e per questo l'educazione della persona digitale (come una sorta di rinnovata educazione civica) deve essere rivolta a tutti i cittadini, agli operatori, agli utenti dello spazio digitale senza distinzione, appunto, di età o di ruoli. Il cambiamento, infatti, non riguarda soltanto le nuove forme espressive e comunicative, ma la stessa struttura della società sempre più digitalizzata nelle sue diverse articolazioni ed organizzazioni.

La svolta indubbiamente positiva imposta dall'Agenda digitale con l'obiettivo di raggiungere elevati livelli di efficienza, razionalizzazione ed economicità, prima di tutto nella pubblica amministrazione, deve essere accompagnata da un quadro giuridico di forti garanzie. L'innovazione, che passa dall'interoperabilità dei sistemi informativi, da un'ampia e agevole disponibilità di informazioni, dalla creazione di nuove banche dati centralizzate, è destinata a riguardare delicati settori: si pensi alla sanità elettronica, di cui il fascicolo sanitario rappresenta l'iniziativa più rilevante, alla giustizia digitale con il processo telematico, all'anagrafe dei conti correnti etc..

La circolazione dei dati personali ha assunto una straordinaria dimensione quantitativa e qualitativa: per questo è necessario uno sforzo imponente delle istituzioni dello Stato per attivare tutte le misure necessarie di natura tecnica (dalla crittografia dei dati alla anonimizzazione) ed organizzativa (dall'autenticazione e tracciabilità degli accessi alla selezione dei dati effettivamente rilevanti) con l'obbiettivo di proteggere la qualità dei dati, garantire la loro sicurezza ed integrità, assicurare l'accesso ai soli soggetti legittimati.

Educazione digitale significa, dunque, anche rendere consapevoli gli operatori che sono impegnati nei progetti ambiziosi di modernizzazione digitale dell'Italia: devono sapere che l'attuazione degli obiettivi si realizza coniugando rigorosi ed elevati standard di sicurezza, qualità e integrità delle diverse banche dati e dei sistemi.

Anche le imprese e gli operatori privati devono sentirsi impegnati ed essere coinvolti i questa sfida.

Proponiamo questo percorso come un progetto unificante, inclusivo, capace di coinvolgere diverse generazioni e interessi, un programma di nuova alfabetizzazione per il diritto di cittadinanza nella società digitale.

L'Autorità di protezione dei dati può rappresentare in questa cornice una frontiera avanzata ed un collaudato punto di incontro dove è possibile ricercare, con tutti gli interlocutori, una sintesi tra efficienza, progresso, rispetto dei diritti e del valore delle persone.

ANTONELLO SORO
Presidente del Garante per la protezione dei dati personali

Le campagne di comunicazione istituzionale del Garante

Il Garante per la privacy è da sempre impegnato nell'attività di informazione e divulgazione con l'obiettivo di far crescere nel nostro Paese una forte cultura della protezione dei dati e promuovere la privacy come diritto fondamentale da tutelare in una società che sia autenticamente democratica.

Questo impegno, che ha riguardato tutti i diversi settori della vita sociale, politica ed economica, è stato ed è rivolto in particolare alle giovani generazioni.

A partire dal vademecum dedicato ai social network del 2009, il Garante ha realizzato campagne di comunicazione istituzionale finalizzate alla sensibilizzazione sui rischi, oltre che sulle opportunità, delle tecnologie digitali, così come sull'uso consapevole delle nuove forme di comunicazione e socializzazione in Rete.

Negli ultimi anni, questa azione di formazione e prevenzione è stata potenziata con il ricorso a strumenti multimediali e prodotti educativi per il web e con l'apertura di appositi spazi dell'Autorità su social network come Youtube e LinkedIn.

Il presente volume raccoglie le principali campagne di comunicazione istituzionale realizzate dall'Autorità e dirette alle famiglie, al mondo delle scuola, alle amministrazioni pubbliche e alle imprese.

SOCIAL NETWORK:
ATTENZIONE AGLI EFFETTI COLLATERALI

Vertigo Design

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.

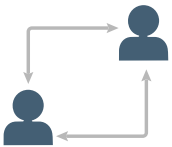

FACEBOOK & CO

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.

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.

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.

LA PRIVACY TRA I BANCHI DI SCUOLA

Vertigo Design

REGOLE GENERALI

VOTI ED ESAMI

INFORMAZIONI
SUGLI STUDENTI

FOTO, AUDIO E VIDEO

SICUREZZA E CONTROLLO

PAROLE CHIAVE

La privacy tra i banchi di scuola

La scuola è chiamata ogni giorno a costruire le condizioni per un futuro migliore delle nuove generazioni.
Non solo nello studio, ma anche nelle esperienze di vita che coinvolgono alunni, professori e personale scolastico si definisce il mondo dei valori che permette alla società di crescere nel rispetto reciproco.

Questa sfida positiva – nella scuola – riguarda anche il "corretto trattamento dei dati personali". Un'espressione che può sembrare asettica, ma che in realtà costituisce una condizione essenziale per il rispetto della dignità delle persone, della loro identità, del loro diritto alla riservatezza.

Nelle scuole, di ogni ordine e grado, vengono trattate giornalmente numerose informazioni sugli studenti e sulle loro famiglie, sui loro problemi sanitari o di disagio sociale, sulle abitudini alimentari. A volte può bastare una lettera contenente dati sensibili (quelli più delicati) su un minorenne, o un tabellone scolastico con riferimenti indiretti sulle condizioni di salute degli studenti, per violare anche involontariamente la riservatezza, la dignità di una persona. Al tempo stesso, "la privacy" è stata talvolta utilizzata in maniera impropria, per non rendere pubbliche determinate informazioni, come i risultati scolastici e quelli degli esami.

Il Garante ritiene utile sgombrare il campo da interpretazioni errate e fornire chiarimenti sulla corretta applicazione della normativa in materia di protezione dei dati personali. Anche allo scopo di sviluppare in ogni componente della comunità scolastica una sempre maggiore consapevolezza dei propri diritti e dei propri doveri.

Questa breve guida propone indicazioni generali tratte da provvedimenti, pareri e note del Garante in tema di privacy a scuola. Per facilitare un agile approfondimento dei vari temi, a conclusione del testo sono segnalati alcuni dei documenti che possono essere consultati sul sito Internet dell'Autorità.

Con il vademecum, il Garante intende offrire un contributo a favore di una comunità scolastica che possa promuovere il rispetto reciproco e tutelare il diritto degli studenti alla riservatezza.


REGOLE
GENERALI

TRATTAMENTO DEI DATI NELLE ISTITUZIONI SCOLASTICHE PUBBLICHE

Le scuole hanno l'obbligo di far conoscere agli studenti e alle loro famiglie – se gli studenti sono minorenni – come usano i loro dati personali. Devono cioè rendere noto, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano. Le scuole pubbliche non sono tenute a chiedere il consenso per il trattamento dei dati personali degli studenti. Gli unici trattamenti permessi sono quelli necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore. Alcune categorie di dati personali degli studenti e delle famiglie – come quelli sensibili e giudiziari – devono essere trattate con estrema cautela, verificando prima non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "rilevanti finalità pubbliche" che si intendono perseguire.

Ad esempio:

ORIGINI RAZZIALI ED ETNICHE

I dati sulle origini razziali ed etniche possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri.

CONVINZIONI RELIGIOSE

Gli istituti scolastici possono utilizzare i dati sulle convinzioni religiose al fine di garantire la libertà di credo – che potrebbe richiedere ad esempio misure particolari per la gestione della mensa scolastica – e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.

STATO DI SALUTE

I dati idonei a rivelare lo stato di salute possono essere trattati per l'assegnazione del sostegno agli alunni disabili; per la composizione delle classi; per la gestione delle assenze per malattia; per l'insegnamento domiciliare e ospedaliero nei confronti degli alunni affetti da gravi patologie; per la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione.

CONVINZIONI POLITICHE

Le opinioni politiche possono essere trattate dalla scuola esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza: ad esempio, le consulte e le associazioni degli studenti e dei genitori.

DATI DI CARATTERE GIUDIZIARIO

I dati di carattere giudiziario possono essere trattati per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione o di protezione. Il trattamento di dati sensibili e giudiziari è previsto anche per tutte le attività connesse ai contenziosi con gli alunni e con le famiglie (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.), e per tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche.

TRATTAMENTO DEI DATI NELLE ISTITUZIONI SCOLASTICHE PRIVATE

Per poter trattare i dati personali le scuole private sono obbligate non solo a presentare un'informativa completa, ma anche a ottenere il consenso puntuale e liberamente espresso dei soggetti interessati (studenti maggiorenni, famiglie...). Nel caso di trattamento di dati giudiziari e sensibili, gli istituti privati sono tenuti a rispettare anche le prescrizioni contenute nelle autorizzazioni generali del Garante, le quali esplicitano i trattamenti consentiti. È possibile, ad esempio, elaborare informazioni sulle convinzioni religiose degli studenti, al fine di permettere la scelta di avvalersi o meno dell'insegnamento della religione cattolica.

DIRITTO DI ACCESSO AI DATI PERSONALI

Anche in ambito scolastico, ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprenderne il contenuto, di farle rettificare se erronee, incomplete o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al "titolare del trattamento" (la scuola) anche tramite suoi incaricati o responsabili. Se non si ottiene risposta, o se il riscontro non è sufficiente, è possibile rivolgersi alla magistratura ordinaria o al Garante.
A tale proposito, è opportuno precisare che l'accesso agli atti amministrativi non è regolato dal Codice della privacy, né vigilato dal Garante per la protezione dei dati personali. Come indicato nella legge n. 241 del 1990 (e successive modifiche) spetta alla singola amministrazione valutare se esistono i presupposti normativi che permettono di prendere visione e di estrarre copia di documenti amministrativi ai soggetti con un "interesse diretto, concreto e attuale" alla conoscibilità degli atti.


VOTI
ED ESAMI
8
7
1/2
6+
9-
3
5
4
10

TEMI IN CLASSE

Non commette violazione della privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale o familiare.
Nel momento in cui gli elaborati vengono letti in classe - specialmente se sono presenti argomenti delicati - è affidata alla sensibilità di ciascun insegnante la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali.
Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto d'ufficio e professionale, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni.

VOTI SCOLASTICI, SCRUTINI, TABELLONI, ESAMI DI STATO

Non esiste alcun provvedimento del Garante che imponga di tenere segreti i voti dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato, perché le informazioni sul rendimento scolastico sono soggette a un regime di trasparenza. Il regime attuale relativo alla conoscibilità dei risultati degli esami di maturità è stabilito dal Ministero dell'istruzione. Per il principio di trasparenza a garanzia di ciascuno, i voti degli scrutini e degli esami devono essere pubblicati nell'albo degli istituti. È necessario prestare attenzione, però, a non fornire – anche indirettamente – informazioni sulle condizioni di salute degli studenti, o altri dati personali non pertinenti. Ad esempio, il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap non va inserito nei tabelloni affissi all'albo dell'istituto, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.

INFORMAZIONI SUGLI STUDENTI

CIRCOLARI E COMUNICAZIONI SCOLASTICHE

Il diritto–dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere sempre bilanciato con l'esigenza di tutelare la personalità dei minori. È quindi necessario, ad esempio, evitare di inserire nelle comunicazioni scolastiche elementi che consentano di risalire, anche indirettamente, all'identità di minori coinvolti in vicende particolarmente delicate.

ORIENTAMENTO, FORMAZIONE E INSERIMENTO PROFESSIONALE

Su richiesta degli studenti interessati, le scuole possono comunicare, anche a privati e per via telematica, i dati relativi ai loro risultati scolastici per aiutarli nell'orientamento, la formazione e l'inserimento professionale anche all'estero.

MARKETING E PUBBLICITÀ

Non è possibile utilizzare i dati presenti nell'albo degli istituti scolastici per inviare materiale pubblicitario a casa degli studenti.
La conoscibilità a chiunque degli esiti scolastici (ad esempio attraverso il tabellone affisso nella scuola) risponde a essenziali esigenze di trasparenza.
Ciò non autorizza soggetti terzi a utilizzare i dati degli studenti per altre finalità come, ad esempio, il marketing e la promozione commerciale.

QUESTIONARI PER ATTIVITÀ DI RICERCA

Svolgere attività di ricerca con la raccolta di informazioni personali, spesso anche sensibili, tramite questionari da sottoporre agli alunni, è consentito soltanto se i ragazzi, o i genitori nel caso di minori, sono stati preventivamente informati sulle modalità di trattamento e conservazione dei dati raccolti e sulle misure di sicurezza adottate. Gli intervistati, inoltre, devono sempre avere la facoltà di non aderire all'iniziativa.

FOTO, AUDIO E VIDEO

RECITE, GITE SCOLASTICHE E FOTO DI CLASSE

Non violano la privacy le riprese video e le fotografie raccolte dai genitori, durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione.
Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare.
In caso di comunicazione sistematica o diffusione diventa, infatti, necessario di regola ottenere il consenso delle persone presenti nelle fotografie e nei video.

REGISTRAZIONE DELLA LEZIONE

È possibile registrare la lezione esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (professori, studenti...), e ottenere il loro esplicito consenso.
Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire gli apparecchi in grado di registrare. (Vedi anche il paragrafo: "Videofonini, filmati, mms")


SICUREZZA E
CONTROLLO

RILEVAMENTO DELLE PRESENZE CON DATI BIOMETRICI

L'utilizzo delle impronte digitali o di altri dati biometrici per rilevare la presenza di un gruppo di individui è giustificato soltanto dall'esistenza di reali esigenze di sicurezza, determinate da concrete e gravi situazioni di rischio. Il sistema di rilevamento delle impronte digitali, ad esempio, è stato giudicato sproporzionato rispetto all'obiettivo di consentire agli studenti l'accesso ai servizi di mensa universitaria.

VIDEOFONINI, FILMATI, MMS

L'utilizzo di videofonini, di apparecchi per la registrazione di suoni e immagini è in genere consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte, in particolare della loro immagine e dignità.
Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori audio-video, inclusi i telefoni cellulari abilitati, all'interno delle aule di lezione o nelle scuole stesse.
Non è possibile, in ogni caso, diffondere o comunicare sistematicamente i dati personali di altre persone (ad esempio immagini o registrazioni audio/video) senza aver prima informato adeguatamente le persone coinvolte e averne ottenuto l'esplicito consenso.

Gli studenti e gli altri membri della comunità scolastica devono quindi prestare particolare attenzione a non mettere on line immagini (ad esempio su blog, siti web, social network) o a diffonderle via mms. Succede spesso, tra l'altro, che una fotografia inviata a un amico/familiare, poi venga inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti.
Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, incorrendo in sanzioni disciplinari, pecuniarie ed eventuali reati.

VIDEOSORVEGLIANZA

L'installazione di sistemi di videosorveglianza nelle scuole deve garantire il diritto dello studente alla riservatezza. In caso di stretta necessità le telecamere sono ammesse, ma devono funzionare solo negli orari di chiusura degli istituti. Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere deve essere opportunamente delimitato. Le immagini registrate possono essere conservate per brevi periodi. Infine, i cartelli che segnalano il sistema di videosorveglianza devono essere visibili anche di notte.

PAROLE CHIAVE

CONSENSO
La libera manifestazione della volontà con la quale, previa idonea informativa, l'interessato accetta in modo esplicito – per iscritto, se vi sono dati sensibili – un determinato trattamento di dati personali che lo riguardano.

DATO PERSONALE
Qualunque informazione relativa a un individuo, a una persona giuridica, a un ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

DATO SENSIBILE
Qualunque dato che può rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'appartenenza a partiti, sindacati o ad associazioni, lo stato di salute e la vita sessuale.

INFORMATIVA
Contiene le informazioni che il titolare del trattamento deve fornire all'interessato per chiarire, in particolare, se quest'ultimo è obbligato o meno a rilasciare i dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione dei dati e in che modo si possono esercitare i diritti riconosciuti dalla legge.

INTERESSATO
La persona cui si riferiscono i dati personali.

TRATTAMENTO
Qualunque operazione effettuata sui dati personali: ad esempio la raccolta, la registrazione, la conservazione, l'elaborazione, l'estrazione, la modifica, l'utilizzo, la diffusione, la cancellazione etc.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

GIORNATA EUROPEA
DELLA PROTEZIONE
DEI DATI PERSONALI

2010
PRIVACY
&CINEMA

Al cinema dal Garante per la Giornata europea della privacy

Al cinema dal Garante, ovvero come utilizzare il cinema per promuovere la tutela della privacy. É l'iniziativa rivolta agli studenti con la quale l'Autorità Garante per la privacy ha deciso di celebrare la Giornata europea della protezione dei dati personali, che cade il 28 gennaio di ogni anno (vedi la pagina del Consiglio d'Europa per informazioni su tutte le iniziative previste).
Obiettivo del progetto, denominato "Cinema & Privacy", è quello di sensibilizzare i giovani sul valore della protezione dei dati personali nella società contemporanea e sulla necessità di imparare a tutelare la propria vita privata.
L'iniziativa prevede - a partire dal 28 gennaio e fino al 2 febbraio presso la Sala Convegni dell'Autorità, in Piazza Monte Citorio 123 - quattro mattine di proiezioni di film che affrontano il tema della privacy sotto diversi aspetti.
Si inizia con "Gattaca", che affronta il tema dell'uso dei dati genetici, per passare a "La finestra sul cortile", sul tema del voyerismo, a "Le vite degli altri", che tratta il tema del controllo totalitario, e finire con "Minority report", su un futuro dominato dalla tecnologia e dai sistemi di sorveglianza.
Alle proiezioni parteciperanno gli studenti di alcune scuole superiori della Capitale chiamati dall'Autorità a discutere e confrontarsi.
Ciascun film verrà introdotto da uno dei quattro Garanti e da un video appositamente realizzato dall'Autorità per raccontare, anche qui con l'aiuto del cinema, le piccole e grandi "invasioni" della nostra sfera privata.
Il video raccoglie infatti spezzoni e sequenze di diversi film che direttamente o indirettamente affrontano i temi della privacy, vista nei suoi aspetti più quotidiani, in quelli più altamente tecnologici, fino a quelli più futuribili e inquietanti.

Comunicato stampa del 26 gennaio 2010

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

2010
PRIVACY
&CINEMA

**GIORNATA EUROPEA
DELLA PROTEZIONE
DEI DATI PERSONALI**

**SALA CONVEGNI
PIAZZA MONTE CITORIO, 123
ROMA**

INIZIO DELLE PROIEZIONI
ORE 9.30

Giovedì **28** gennaio
GATTACA

Venerdì **29** gennaio
LA FINESTRA SUL CORTILE

Lunedì **1** febbraio
LE VITE DEGLI ALTRI

Martedì **2** febbraio
MINORITY REPORT

www.garanteprivacy.it

DALLA PARTE
DEL PAZIENTE

PRIVACY: LE DOMANDE PIÙ FREQUENTI

Vertigo Design


IL PAZIENTE INFORMATO
INFORMAZIONI SULLA SALUTE
IN ATTESA
TELECAMERE E INTERNET
LA SALUTE DEI DIPENDENTI
HIV
SANITÀ ELETTRONICA
I TERMINI PIÙ USATI

Dalla parte del paziente

Alle persone che entrano in contatto con medici e strutture sanitarie per cure, prestazioni mediche, acquisto di medicine, operazioni amministrative, devono essere garantite la più assoluta riservatezza e il rispetto della dignità.
I dati personali in grado di rivelare lo stato di salute delle persone sono infatti di particolare delicatezza, per questo definiti "dati sensibili", e non possono essere diffusi. Ad essi il Codice sulla protezione dei dati personali attribuisce una tutela rafforzata e stabilisce le regole per il loro trattamento in ambito sanitario, tenendo sempre conto del ruolo professionale dei medici e del personale paramedico.

Questa guida raccoglie le risposte alle domande più frequenti che vengono poste all'attenzione dell'Autorità da pazienti e personale sanitario offrendo anche un quadro delle principali indicazioni fornite dal Garante nel corso del tempo. L'intento è quello di agevolare le attività degli operatori del settore e di contribuire a migliorare le condizioni di vita quotidiana di chi accede a farmacie, studi medici, ospedali e a qualunque altro luogo di analisi o cura.
Chi volesse approfondire gli aspetti legati alla tutela della privacy in ambito sanitario può consultare il Codice della privacy, la documentazione e i provvedimenti pubblicati sul sito internet **www.garanteprivacy.it** oppure può contattare direttamente gli uffici del Garante.

IL PAZIENTE INFORMATO

OCCORRE CHIEDERE IL CONSENSO AL PAZIENTE PRIMA DI ACQUISIRE E UTILIZZARE INFORMAZIONI SULLA SUA SALUTE?

Sì. Gli organismi sanitari pubblici e privati (ospedali, case di cura...), come pure gli esercenti le professioni sanitarie (farmacisti, medici, infermieri..), devono fornire al paziente una informativa sul trattamento dei dati personali che lo riguardano e acquisire il consenso al loro uso.

... E SE IL PAZIENTE NON È IN GRADO DI DARE IL CONSENSO AL TRATTAMENTO DEI DATI, MA DEVE ESSERE SOTTOPOSTO A CURE?

Non è necessario dare un previo consenso all'uso dei dati nei casi di rischio imminente per la salute, o quando vi è impossibilità fisica o incapacità di agire, di intendere o di volere del paziente. In questi casi il consenso al trattamento dei dati personali può essere espresso, se ne è in grado, dal paziente stesso, successivamente alla prestazione sanitaria ricevuta, o da un terzo (ad esempio un familiare, un convivente, un responsabile della struttura presso cui dimora).

QUALI INFORMAZIONI DEVONO ESSERE FORNITE AL PAZIENTE?

L'informativa data all'interessato deve indicare chi è il soggetto (ad esempio il medico) che raccoglie i suoi dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione

dei dati e se il paziente
è obbligato o meno a fornirli.
Deve contenere anche indicazioni
sulle modalità con cui la persona
interessata può esercitare i diritti
riconosciuti dalla legge, come la
richiesta di integrazione, aggiornamento
o cancellazione dei dati trattati.

L'INFORMATIVA DEVE SEMPRE ESSERE FORNITA IN FORMA SCRITTA?

No, l'informativa può essere data una tantum anche oralmente. È comunque preferibile che venga fornita per iscritto, magari attraverso un pieghevole, oppure affiggendone il testo in un luogo facilmente visibile, come nella sala d'attesa dell'ambulatorio.

Il Garante ha predisposto un modello semplificato di informativa per i medici di famiglia e i pediatri.
Tale informativa, se non è diversamente specificato, vale anche per i trattamenti correlati, come ad esempio quello effettuato dal medico specialista cui è stato richiesto un accertamento specifico, o dal farmacista che fornisce il medicinale.

INFORMAZIONI SULLA SALUTE

PUÒ IL MEDICO INFORMARE ALTRE PERSONE SULLO STATO DI SALUTE DI UN SUO ASSISTITO?

È possibile, ma il paziente deve aver indicato a chi desidera che siano fornite tali informazioni.

SE UNA PERSONA VIENE PORTATA AL PRONTO SOCCORSO O RICOVERATA, CHI PUÒ AVERE NOTIZIE?

L'organismo sanitario può dare informazioni, anche per telefono, sulla presenza di una persona al pronto soccorso o sui degenti presenti nei reparti solo ai terzi legittimati, come parenti, familiari, conviventi, conoscenti, personale volontario. L'interessato, se cosciente e capace, deve essere preventivamente informato (ad esempio al momento dell'accettazione) e poter decidere a chi possono essere comunicate notizie sulla propria salute. Occorre comunque rispettare l'eventuale richiesta della persona ricoverata a non rendere note neppure ai terzi legittimati la sua presenza nella struttura sanitaria o le informazioni sulle sue condizioni di salute.

LE ASSOCIAZIONI DI VOLONTARIATO POSSONO RICEVERE INFORMAZIONI SUI LORO ASSISTITI?

Sì, ma devono osservare tutte le regole che le strutture sanitarie prevedono per il proprio personale interno al fine di garantire il rispetto della dignità della persona e il massimo livello di tutela dei pazienti, nonché il segreto professionale.

L'ESITO DELLE ANALISI O LE CARTELLE CLINICHE DA CHI POSSONO ESSERE RITIRATI?

I referti diagnostici, le cartelle cliniche, i risultati delle analisi e i certificati rilasciati dagli organismi sanitari possono essere consegnati in busta chiusa anche a persone diverse dai diretti interessati purché munite di delega scritta.

È POSSIBILE CONOSCERE I DATI CONTENUTI NELLA CARTELLA CLINICA DI UN DEFUNTO?

Può accedere ai dati personali del defunto chi abbia un interesse proprio, o agisca a tutela della persona deceduta o per ragioni familiari meritevoli di protezione.

IN ATTESA

A CHE SERVE LA "DISTANZA DI CORTESIA"?

Per garantire la riservatezza dei colloqui. Presso gli sportelli di ospedali e delle aziende sanitarie o nelle farmacie devono essere previsti appositi spazi - spesso segnalati con una riga gialla - oltre i quali gli utenti possano attendere il proprio turno.

NELLE SALE D'ASPETTO IN CHE MODO IL PAZIENTE DEVE ESSERE AVVISATO DEL PROPRIO TURNO?

Nei locali di grandi strutture sanitarie i nomi dei pazienti in attesa di una prestazione o di documentazione (ad esempio delle analisi cliniche) non devono essere divulgati ad alta voce. Occorre adottare soluzioni alternative: per esempio, attribuendo un codice alfanumerico al momento della prenotazione o dell'accettazione.

... E QUANDO SI È DAL MEDICO DI BASE?

I medici di base, gli studi medici privati e i medici specialisti che hanno un rapporto personalizzato con i loro assistiti, possono chiamarli per nome.

ALL'INGRESSO DEI REPARTI POSSONO ESSERE AFFISSE LE LISTE DEI PAZIENTI IN ATTESA DI UN INTERVENTO?

No. Non è giustificata l'affissione di liste di pazienti in attesa di intervento in locali aperti al pubblico, con o senza la descrizione della patologia sofferta. Non devono essere resi visibili ad estranei neanche documenti sulle condizioni cliniche del malato, come le cartelle infermieristiche poste vicino al letto di degenza.

QUALI PRECAUZIONI DEVE ADOTTARE IL PERSONALE SANITARIO PER TUTELARE LA PRIVACY DEI PAZIENTI?

Il personale sanitario deve evitare che le informazioni sulla salute possano essere conosciute da soggetti non autorizzati, a causa di situazioni di promiscuità derivanti dall'organizzazione dello spazio dei locali o dalle modalità utilizzate. Il Garante ha prescritto a questo scopo specifici accorgimenti per garantire la riservatezza dei pazienti sia durante l'orario di visita, sia all'atto della prescrizione di ricette mediche o del rilascio di certificati. Tra questi accorgimenti va ricordato, ad esempio, l'uso di paraventi o simili nei reparti di rianimazione, volti a limitare la visibilità del malato ai soli familiari e conoscenti.

TELECAMERE E INTERNET

POSSONO ESSERE INSTALLATE DELLE TELECAMERE IN OSPEDALI E LUOGHI DI CURA?

L'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari locali (ad esempio nelle unità di rianimazione o in reparti di isolamento) devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati.

CHI PUÒ VEDERE LE IMMAGINI RIPRESE NEI LUOGHI DI CURA?

La visione delle immagini deve essere consentita solo al personale autorizzato (ad esempio a medici e infermieri) e ai familiari dei ricoverati (familiari, parenti, conoscenti). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video di ricoverati in reparti dove non sia consentito a parenti e amici di recarsi personalmente (ad esempio in rianimazione): a questi ultimi può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell'immagine solo del proprio congiunto o conoscente. Non bisogna quindi collocare i monitor in locali liberamente accessibili al pubblico. La diffusione di immagini idonee a rivelare lo stato di salute è infatti vietata.

IL PAZIENTE PUÒ OTTENERE LA COPIA DELLA REGISTRAZIONE VIDEO DEL PROPRIO INTERVENTO?

L'interessato ha diritto di accedere a tutti i dati personali che lo riguardano, in qualunque documento, supporto anche visivo o archivio essi siano contenuti,

senza dover fornire giustificazioni della necessità di ottenere tali informazioni. Può così accedere anche alle fotografie scattate prima e dopo gli interventi chirurgici e chiederne copia, così come può ottenere il video dell'operazione e ogni altra informazione che lo riguardi.

L'ELENCO DEI DEGENTI DI UN OSPEDALE PUÒ ESSERE PUBBLICATO SUL WEB?

È vietata la diffusione di dati idonei a rivelare lo stato di salute. Non possono quindi essere resi disponibili a chiunque su internet i dati anagrafici, l'indicazione delle diagnosi o i risultati delle analisi cliniche delle persone che si recano presso un ospedale.

È POSSIBILE CARICARE FOTO O ALTRE INFORMAZIONI RELATIVE A DEGENTI SULLA PROPRIA PAGINA DI FACEBOOK O DI ALTRI SOCIAL NETWORK?

Attenzione a non pubblicare dati personali, ad esempio nomi o fotografie,

di pazienti sulle proprie pagine di social network. Anche se spesso si pensa di condividerle solo con amici, magari colleghi sanitari, si rischia invece di diffonderle a un numero imprecisato di utenti della rete, violando così la privacy delle persone coinvolte.

LE GRADUATORIE DEI DISABILI BENEFICIARI DI UN CONTRIBUTO PUBBLICO POSSONO ESSERE DIVULGATE SU SITI INTERNET DELLA PUBBLICA AMMINISTRAZIONE?

È sempre vietato diffondere informazioni sulla salute di una persona. Senza venir meno al principio della trasparenza, la pubblica amministrazione deve evitare di pubblicare oltre alla lista dei beneficiari di contributi o di altre agevolazioni anche ulteriori informazioni delicate, quali il tipo di patologia associata al singolo individuo.

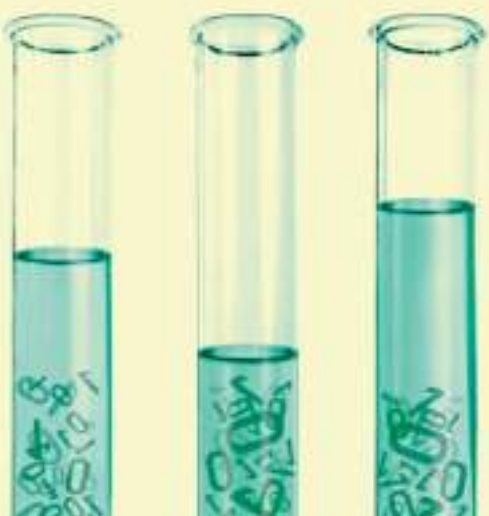
LA SALUTE DEI DIPENDENTI

IL DATORE DI LAVORO PUÒ CHIEDERE CHE NEI CERTIFICATI MEDICI SIA INDICATA LA DIAGNOSI DELLA MALATTIA DEL DIPENDENTE?

Il datore di lavoro non è legittimato a raccogliere certificati di malattia dei dipendenti con l'indicazione della diagnosi. In assenza di specifiche deroghe previste da leggi o regolamenti, il lavoratore assente per malattia deve fornire un certificato contenente esclusivamente la prognosi con la sola indicazione dell'inizio e della durata dell'infermità.

QUALI INFORMAZIONI DEVONO ESSERE CONTENUTE NEI CERTIFICATI MEDICI CHE ATTESTINO L'IDONEITÀ AL SERVIZIO?

Nei certificati medici legali che attestano l'idoneità al servizio di un lavoratore, deve essere riportato il solo giudizio medico legale senza diagnosi, anziché il verbale integrale della visita collegiale.



IL DATORE DI LAVORO PUÒ PUBBLICARE INFORMAZIONI SULLA SALUTE DEI PROPRI DIPENDENTI?

Sia le imprese private, sia la pubblica amministrazione devono tutelare con la massima diligenza le informazioni sulla salute dei propri dipendenti, così come quelle dei dirigenti, evitando che vengano divulgate. L'utilizzo ingiustificato di questi dati può creare disagio alla persona o esporla a conseguenze indesiderate.

HIV

IL MEDICO PUÒ CHIEDERE AL SUO PAZIENTE SE È SIEROPOSITIVO?

Coloro che esercitano la professione sanitaria non possono raccogliere, al momento dell'accettazione, informazioni sulla sieropositività del paziente che si rivolge allo studio medico, a meno che ciò non risulti indispensabile per il tipo di intervento o terapia che si deve eseguire.
In ogni caso, il dato sull'infezione da Hiv (virus dell'immunodeficienza) deve essere raccolto direttamente dal medico, non dal personale amministrativo e sempre con il consenso del paziente.

IN QUESTO CASO, COME SI CONCILIA LA TUTELA DELLA PRIVACY CON LA SICUREZZA DEL PERSONALE MEDICO?

La normativa di settore prevede che siano adottate specifiche misure di protezione dal contagio nei confronti di ogni paziente, a prescindere dalla conoscenza dello stato di sieropositività. L'esigenza di ottenere informazioni sull'infezione da Hiv fin dal momento dell'accettazione non può dunque essere giustificata dalla necessità di attivare tali misure. Nel caso in cui il medico venga a conoscenza di un caso di Aids o di Hiv, oltre a rispettare specifici obblighi di segretezza e non discriminazione nei confronti del paziente, ha l'obbligo di adottare ogni misura individuata dal Codice della privacy per garantire la sicurezza dei dati sanitari.

SANITÀ ELETTRONICA

IL PAZIENTE È OBBLIGATO AD ADOTTARE IL FASCICOLO SANITARIO ELETTRONICO?

No. Il paziente deve poter scegliere, in piena libertà, se far costituire o meno un fascicolo sanitario elettronico (Fse), con tutte o solo alcune delle informazioni sanitarie che lo riguardano.
Deve quindi ricevere un'adeguata informativa che chiarisca chi (medici di base, del reparto ove è ricoverato, farmacisti...) ha accesso ai suoi dati e come possono essere utilizzati.
E deve poter manifestare un consenso autonomo e specifico, distinto da quello che si presta a fini di cura della salute.
Al paziente deve essere inoltre garantita la possibilità di "oscurare" la visibilità di alcuni eventi clinici. Se il paziente non vuole aderire al Fse deve comunque poter usufruire delle prestazioni del servizio sanitario nazionale.

CHI PUÒ ACCEDERE AL FASCICOLO SANITARIO ELETTRONICO?

Il fascicolo sanitario elettronico può essere consultato dal paziente con modalità adeguate (ad esempio tramite smart card) e dal personale sanitario strettamente autorizzato per finalità sanitarie (prevenzione, diagnosi, cura e riabilitazione dell'interessato).
Non potranno accedervi invece periti, compagnie di assicurazione, datori di lavoro.

I REFERTI MEDICI POSSONO ESSERE INVIATI ALL'ASSISTITO TRAMITE INTERNET?

Sì. I risultati di analisi cliniche, radiografie e referti medici possono essere inviati direttamente sulla e-mail del paziente o possono essere resi consultabili on line dal computer di casa. L'adesione al servizio dovrà però essere facoltativa e il referto cartaceo rimarrà comunque disponibile.

L'assistito dovrà dare il suo consenso sulla base di una informativa chiara e trasparente che spieghi tutte le caratteristiche del servizio di consultazione o consegna on line dei referti.
Le strutture che offrono la possibilità di archiviare e continuare a consultare via web i referti dovranno fornire una ulteriore specifica informativa e acquisire un autonomo consenso.

QUANTO TEMPO POTRANNO ESSERE CONSERVATI ON LINE I REFERTI?

Il referto potrà rimanere consultabile on line solo per un periodo di tempo limitato di quarantacinque giorni. Dovrà inoltre essere accompagnato da un giudizio scritto e dalla disponibilità del medico a fornire ulteriori indicazioni su richiesta del paziente.

I TERMINI PIÙ USATI

TRATTAMENTO DEI DATI PERSONALI
Qualunque operazione effettuata sui dati: ad esempio, la raccolta, la registrazione, la conservazione, l'elaborazione, l'estrazione, la modificazione, l'utilizzo, la diffusione, la cancellazione etc.

DATO PERSONALE
Qualunque informazione relativa ad una persona.

DATO SENSIBILE
Qualunque dato che può rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'appartenenza a partiti, sindacati o ad associazioni, lo stato di salute e la vita sessuale dell'interessato.

INTERESSATO
La persona cui si riferiscono i dati personali.

INFORMATIVA
Contiene le informazioni che il titolare del trattamento (ad esempio: ospedale, farmacia, medico..) deve fornire all'interessato per chiarire, in particolare, se quest'ultimo è obbligato o meno a fornire i dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione dei dati e in che modo si possono esercitare i diritti riconosciuti dalla legge.
Il Garante ha predisposto un modello semplificato di informativa che può essere utilizzato dai medici di famiglia e dai pediatri.

CONSENSO
Autorizzazione al trattamento dei propri dati personali rilasciata dall'interessato.

FASCICOLO SANITARIO ELETTRONICO

È un documento elettronico che contiene i dati sanitari di ogni paziente, quali patologie, interventi chirurgici, esami clinici, farmaci prescritti, documentazione sui ricoveri.
È consultabile on line sia dall'interessato, sia da altri soggetti eventualmente autorizzati.
È aggiornabile da medici, farmacisti, enti ospedalieri.

SOCIAL NETWORK

I social network (Facebook, Twitter e altri) sono "piazze virtuali", cioè dei luoghi in cui via internet ci si ritrova portando con sé e condividendo on line fotografie, filmati, pensieri, indirizzi di amici e tante altre informazioni.

DI CHE PARLIAMO QUANDO PARLIAMO DI PRIVACY?
CHE NE SAI DAVVERO DEI SOCIAL NETWORK?

TROVA LA RISPOSTA, PARTECIPA AL CONCORSO
E GIRA IL TUO CORTOMETRAGGIO

privacy2.0

Realizza un "corto" sulla privacy. Il Garante privacy lancia un concorso per gli studenti delle scuole superiori

Di che parliamo quando parliamo di privacy? Quale idea ne hanno i giovani che usano in maniera disinvolta cellulari di nuova generazione e Internet? Quanto sanno davvero che cos'è un social network?
A queste e ad altre questioni sono chiamati a dare risposta gli studenti delle scuole superiori italiane che il Garante per la privacy ha voluto coinvolgere con il concorso "Privacy 2.0 - I giovani e le nuove tecnologie", organizzato in collaborazione con Guida Monaci. E dovranno farlo girando un "corto" e trasformandosi per una volta in sceneggiatori, attori, registi.
Il Garante vuole infatti che siano i ragazzi a realizzare, attraverso i loro video, una sorta di "campagna di informazione" per sensibilizzare la nostra società sulla protezione dei dati personali.
Il concorso prevede che gli studenti, che frequentano le terze e quarte classi delle scuole sorteggiate per ogni provincia italiana, girino un video originale di tre minuti scegliendo un tema, un aspetto, un fenomeno legati alla protezione dei dati in rapporto alle nuove tecnologie.
Gli studenti potranno realizzare il "corto" da soli o in gruppo, assistiti o meno da un insegnante. I video dovranno arrivare presso la sede del Garante entro il 30 ottobre 2011. Una giuria di esperti selezionerà i lavori. Al video vincitore andrà un premio di 5.000 euro. Alle scuole sorteggiate verrà distribuito materiale illustrativo utile per la partecipazione al concorso. Tutta la documentazione sarà consultabile sul sito del Garante www.garanteprivacy.it/concorsoscuole e sul sito di Guida Monaci www.guidamonaci.it/garanteprivacy.
La premiazione avverrà il 28 gennaio 2012, in occasione della Giornata Europea della protezione dei dati.

Comunicato stampa del 14 aprile 2011

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

GUIDA MONACI

DI CHE PARLIAMO QUANDO PARLIAMO DI PRIVACY? CHE NE SAI DAVVERO DEI SOCIAL NETWORK?

TROVA LA RISPOSTA, PARTECIPA AL CONCORSO E GIRA IL TUO CORTOMETRAGGIO

privacy2.0

Internet, cellulari, servizi on line, mappe per conoscere la posizione degli amici semplificano la nostra vita e ci permettono di rimanere costantemente in contatto, ma possono determinare anche dei grandi rischi per la nostra sfera privata. Il Garante per la protezione dei dati personali in collaborazione con la Guida Monaci ha indetto il Concorso "Privacy2.0 - I giovani e le nuove tecnologie" per sensibilizzare le nuove generazioni su un tema così importante. Il Concorso prevede la realizzazione di un cortometraggio da parte degli studenti delle scuole superiori che frequentano le classi III e IV dell'anno scolastico 2010-2011. Ogni istituto potrà inviare fino a tre cortometraggi che dovranno pervenire al Garante **entro e non oltre il 30.10.2011**. Un'apposita giuria premierà i tre lavori migliori. Al primo classificato andrà un premio di **€ 5.000**. Sono previsti premi anche per la scuola.

>>> Per saperne di più contatta l'ufficio di presidenza della tua scuola

oppure vai sul sito www.garanteprivacy.it/concorsoscuole

Ad un liceo di Taranto il primo premio per un "corto" sulla privacy.

Gli studenti premiati oggi dal Garante in occasione della Giornata europea della protezione dei dati personali

"Proteggi il tuo mondo!" è il titolo del "corto" del Liceo "Galileo Ferraris" di Taranto che ha vinto i 5.000 euro del Concorso "Privacy 2.0 - I giovani e le nuove tecnologie", indetto dal Garante per la protezione dei dati personali nel 2011, in collaborazione con Guida Monaci che ha curato la parte organizzativa, rivolto alle ultime classi delle scuole superiori. Al secondo posto si è classificato il video "Pubblica intimità" realizzato dagli studenti del Liceo "Amaldi" di Novi Ligure, mentre al terzo posto è giunto "Vite inscatolate" dell'Istituto Magistrale "Renier" di Belluno.

I tre filmati, selezionati da una apposita giuria presieduta da Giuseppe Chiaravalloti vice presidente dell'Autorità garante, sono stati premiati oggi in occasione della Giornata europea della protezione dei dati personali. Ai ragazzi era stato chiesto di trasformarsi per una volta in sceneggiatori, attori, registi e di "girare" un video sulla protezione dei dati personali in rapporto all'uso della rete e alle nuove tecnologie.

"Nella scelta dei vincitori la Giuria - si legge nella motivazione - ha privilegiato l'aderenza del messaggio ai valori della privacy, l'immediatezza e l'efficacia simbolica del linguaggio usato, tenuto conto anche della qualità tecnica dei filmati".

Targhe ricordo e premi sono stati consegnati anche alle scuole alle quali appartengono gli autori dei video che hanno sostenuto i ragazzi nell'impegno di confrontarsi con un tema, così rilevante nella nostra società, come quello della privacy."Profonda soddisfazione" - è stata espressa dal presidente del Garante Francesco Pizzetti - "per la partecipazione e la sensibilità dimostrata dagli studenti nell'affrontare le tematiche proposte e per la qualità generale dei cortometraggi inviati dalle scuole. Il dialogo con le nuove generazioni e il loro contributo al dibattito - ha aggiunto Pizzetti - assumono ancora più valore proprio nel momento in cui l'Europa sta rafforzando le garanzie a tutela degli utenti nel mondo on line".

Alla premiazione hanno preso parte anche Mauro Paissan componente dell'Autorità, e Stefano Zapponini presidente di Guida Monaci, che hanno avuto parole di elogio e di apprezzamento verso i premiati.

Comunicato stampa del 28 gennaio 2012

I video vincitori

1° - Proteggi il tuo mondo!

2°- Pubblica intimità

3°- Vite inscatolate

CLOUD COMPUTING

PROTEGGERE I DATI
PER NON CADERE DALLE NUVOLE

Mini guida per imprese
e pubblica amministrazione

Vertigo Design


COS'È IL
CLOUD COMPUTING
NUVOLE DIVERSE
PER ESIGENZE DIVERSE
IL QUADRO
GIURIDICO
VALUTAZIONE DEI RISCHI,
DEI COSTI E DEI BENEFICI
IL DECALOGO PER UNA
SCELTA CONSAPEVOLE

CLOUD COMPUTING

PROTEGGERE I DATI
PER NON CADERE DALLE NUVOLE

Ogni imprenditore, ma anche ogni attento amministratore pubblico, si adopera per offrire, rispettivamente ai propri clienti e ai cittadini, servizi migliori a minor costo. Le tecnologie informatiche, in particolare quelle del cloud computing, garantiscono oggi soluzioni innovative per gestire molteplici attività con efficienza e possibili risparmi. Ma presentano criticità e rischi per la privacy di cui è bene tenere conto. Prima di esternalizzare la gestione di dati e documenti o adottare nuovi modelli organizzativi è necessario porsi alcune domande, scegliendo con cura la soluzione più sicura per le attività istituzionali o per il proprio business. Con questo vademecum, il Garante per la protezione dei dati personali intende offrire alcune indicazioni valide per tutti gli utenti, in particolare imprese e amministrazioni pubbliche. L'obiettivo è quello di far riflettere su alcuni importanti aspetti giuridici, economici e tecnologici in un settore in velocissima espansione e di promuovere un utilizzo corretto delle nuove modalità di erogazione dei servizi informatici.


COS'È IL CLOUD
COMPUTING

Con il termine cloud computing, o semplicemente cloud, ci si riferisce a un insieme di tecnologie e di modalità di fruizione di servizi informatici che favoriscono l'utilizzo e l'erogazione di software, la possibilità di conservare e di elaborare grandi quantità di informazioni via Internet.
Il cloud offre, a seconda dei casi, il trasferimento della conservazione o dell'elaborazione dei dati dai computer degli utenti ai sistemi del fornitore.
Il cloud consente, inoltre, di usufruire di servizi complessi senza doversi necessariamente dotare né di computer e altri hardware avanzati, né di personale in grado di programmare o gestire il sistema.

Tutto può essere demandato all'esterno, in *outsourcing*, e a un costo potenzialmente limitato, in quanto le risorse informatiche necessarie per i servizi richiesti possono essere condivise con altri soggetti che hanno le stesse esigenze.

L'AUTOMOBILE "INFORMATICA" E IL CLOUD PER PROFANI

Opzione 1 – tutto in casa:
se una persona o una società ha bisogno di un'automobile può progettarla, acquistarne le singole componenti e assemblarle, nonché attrezzare all'interno della propria casa o della propria sede un'officina con personale specializzato per le riparazioni e la manutenzione.

Opzione 2 – intervento esterno:
si può decidere di acquistare l'automobile e di portarla in caso di necessità da un meccanico di fiducia, di affittarla, di prenderla in leasing, di chiamare un taxi o noleggiare una vettura con autista. La scelta tra queste opzioni è determinata dal tipo di utilizzo che si vuole fare dell'autoveicolo, dalla frequenza con cui se ne fruisce, dalle prestazioni che eventualmente si desiderano e, comunque, dalle risorse economiche a disposizione.

Con il cloud computing ci troviamo in questa seconda opzione.
Non parliamo di automobili o altri mezzi di trasporto ma di servizi informatici. Le soluzioni offerte dal cloud generalmente possono essere più flessibili, efficienti, adattabili ed economiche di quelle sviluppate *in-house* (in casa propria).
Ma possono comportare il rischio di una potenziale perdita di controllo sui propri dati.

Spesso utilizziamo tecnologie cloud senza neppure saperlo. Alcuni dei più diffusi servizi di posta elettronica o di elaborazione testi sono "sulle nuvole". Anche molte delle funzioni offerte dai cellulari di nuova generazione (i cosiddetti smartphone) sono basate sul cloud: ad esempio quelle che sfruttano la geolocalizzazione consigliandoci i locali o gli esercizi commerciali più vicini, che consentono di ascoltare musica o di accedere a giochi on line, nonché tante altre funzioni e "app"(applicazioni).


NUVOLE DIVERSE
PER ESIGENZE
DIVERSE

Esistono vari tipi di cloud computing, classificati sia in base all'architettura della "nuvola" e alla gestione interna o esterna del trattamento dati, sia in relazione al modello di servizio offerto al cliente. Ogni tipo di cloud ha le sue caratteristiche peculiari che dovranno essere ben valutate dalle società e dalle pubbliche amministrazioni che intendono servirsi delle "nuvole".

TIPI DI CLOUD

Private Cloud
La "nuvola privata" è una infrastruttura informatica (rete di computer collegati per offrire servizi) per lo più dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo (nella tradizionale forma dell'hosting dei server), nei confronti del quale il titolare dei dati può esercitare un controllo puntuale. Le "nuvole private" possono essere paragonate ai tradizionali "data center" nei quali, però, sono usati degli accorgimenti tecnologici che permettono di ottimizzare l'utilizzo delle risorse disponibili e di potenziarle agevolmente in caso di necessità.

Public Cloud
Nel caso della "nuvola pubblica", l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni i propri sistemi attraverso la condivisione e l'erogazione via Internet di applicazioni informatiche, di capacità elaborativa e di "stoccaggio" dati. La fruizione di tali

servizi avviene tramite la rete Internet e implica il trasferimento dei soli dati o anche dell'attività di elaborazione presso i sistemi del fornitore del servizio, il quale assume un ruolo importante in ordine all'efficacia delle misure adottate per garantire la protezione delle informazioni che gli sono state affidate. Con il cloud pubblico l'utente insieme ai dati, infatti, cede una parte importante del controllo esercitabile su di essi.

Altre "nuvole"
Esistono altri tipi di nuvole con caratteristiche miste, quali i cloud ibridi (*hybrid cloud*) - caratterizzati da soluzioni che prevedono l'utilizzo di servizi erogati da infrastrutture private accanto a servizi acquisiti da cloud pubblici - e i cloud di gruppo (*community cloud*), in cui l'infrastruttura è condivisa da diverse organizzazioni a beneficio di una specifica comunità di utenti.

TRE MODELLI DI SERVIZI CLOUD

Cloud Infrastructure as a Service - IaaS
(infrastruttura cloud resa disponibile come servizio)
Il fornitore del servizio cloud offre, secondo un modello "a consumo", gli strumenti hardware e software di base

(spazi di memoria, sistemi operativi, programmi di virtualizzazione...), cioè server virtuali remoti che l'utente finale può utilizzare in sostituzione o in affiancamento ai sistemi già presenti nei locali dell'azienda o dell'amministrazione. Tali fornitori sono in genere operatori di mercato specializzati, che dispongono di un'infrastruttura tecnologica, complessa e spesso distribuita in aree geografiche diverse.

Cloud Software as a Service - SaaS
(software erogato come servizio del cloud)
Il fornitore eroga via Internet una serie di servizi applicativi ponendoli a disposizione degli utenti finali. Si pensi, ad esempio, ad applicazioni comunemente usate negli uffici erogate in modalità web quali l'elaborazione di fogli di calcolo o di testi, la gestione del protocollo e delle regole per l'accesso informatico ai documenti, la rubrica dei contatti e i calendari condivisi, ma anche ai più avanzati servizi di posta elettronica.

Cloud Platform as a Service - PaaS
(piattaforme software fornite via Internet come servizio)
Il fornitore offre soluzioni evolute di sviluppo software che rispondono alle specifiche esigenze del cliente. In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie (ad esempio applicativi per la gestione finanziaria, della contabilità o della logistica), allo scopo di assolvere a esigenze interne, oppure per fornire a loro volta servizi a terzi. Anche nel caso dei *PaaS,* il servizio erogato dal fornitore limita la necessità per il fruitore di doversi dotare internamente di strumenti hardware o software specifici o aggiuntivi.


IL QUADRO
GIURIDICO

LA SFIDA INTERNAZIONALE

La tecnologia cloud procede molto più velocemente dell'attività del legislatore, non solo in Italia ma in tutto il mondo. Manca ancora un quadro normativo aggiornato – in tema di privacy, ma anche in ambito civile e penale - che tenga conto di tutte le novità introdotte dal cloud computing e sia in grado di offrire adeguate tutele nei riguardi delle fattispecie giuridiche connesse all'adozione di servizi distribuiti di elaborazione e di conservazione dati. Basti pensare, ad esempio, che la normativa europea sulla protezione dei dati risale al 1995.
Alcune utili novità per il settore delle telecomunicazioni, che avranno un indubbio impatto anche sul cloud, sono state introdotte dal cosiddetto "pacchetto Telecom": in particolare dalla direttiva 136/2009 - attualmente in corso di recepimento da parte degli Stati membri dell'Ue – che modifica la direttiva sulla privacy nelle comunicazioni elettroniche del 2002. Fra le misure che entreranno in vigore con il nuovo quadro giuridico è previsto anche l'obbligo per le società telefoniche e gli Internet provider di notificare alle competenti Autorità nazionali e, in determinati casi, agli utenti, tutte le violazioni di sicurezza che comportino la distruzione, la perdita o la diffusione indebita di dati personali trattati nell'ambito della fornitura del servizio.
Un ulteriore importante cambiamento per tutto il settore delle comunicazioni elettroniche, e del cloud computing in particolare, dovrebbe avvenire entro il 2014, con l'approvazione del nuovo Regolamento generale sulla protezione dei dati (Com 2012 11 def) proposto

dalla Commissione Europea.
Il nuovo Regolamento introdurrà identiche regole in Europa e nei confronti di Stati terzi (riscrivendo quindi anche il Codice della privacy italiano), e in questo senso dovrebbe contribuire a rendere meno complesso e rischioso l'utilizzo di servizi cloud. Una delle importanti innovazioni di questa riforma riguarderà l'estensione dell'obbligo di notifica delle violazioni di sicurezza che riguardino dati personali a tutti i titolari del trattamento dati come, ad esempio, banche, assicurazioni, Asl, enti locali. Quando previsto, le persone interessate saranno quindi informate senza ritardo della perdita o del furto dei loro dati.

NORMATIVA PRIVACY NELLE NUVOLE – SPUNTI DI RIFLESSIONE

In attesa di una normativa nazionale e internazionale aggiornata e uniforme, che permetta di governare il fenomeno senza rischiare di penalizzare l'innovazione e le potenzialità di sviluppo delle "nuvole" informatiche, è necessario che le imprese e la pubblica amministrazione, incluse tra l'altro le cosiddette "centrali di committenza" (soggetti che effettuano acquisti per una pluralità di pubbliche amministrazioni), prestino particolare attenzione ai rischi connessi all'adozione dei servizi di cloud computing, anche in relazione agli aspetti di protezione dei dati personali.

Il titolare e il responsabile del trattamento

La pubblica amministrazione o l'azienda, "titolare del trattamento" dei dati personali, che trasferisce del tutto o in parte il trattamento sulle "nuvole", deve procedere a designare il fornitore dei servizi cloud "responsabile del trattamento".

Questo significa che il cliente dovrà sempre prestare molta attenzione a come saranno utilizzati e conservati i dati personali caricati sulla "nuvola": in caso di violazioni commesse dal fornitore, anche il titolare sarà chiamato a rispondere dell'eventuale illecito.
Il cliente di ridotte dimensioni, come una piccola impresa o un ente locale, potrebbe tuttavia incontrare difficoltà nel contrattare adeguate condizioni per la gestione dei dati spostati "sulla nuvola". Anche in questo caso, non sarà però sufficiente, per giustificare una eventuale violazione, affermare di non avere avuto possibilità di negoziare clausole contrattuali o modalità di controllo più stringenti. Il cliente di servizi cloud, infatti, può sempre rivolgersi ad altri fornitori che offrono maggiori garanzie, in particolare per il rispetto della normativa sulla protezione dei dati. Il Codice della privacy prevede,

tra l'altro, che il titolare eserciti un potere di controllo nei confronti del responsabile del trattamento (in questo caso il cloud provider), verificando la corretta esecuzione delle istruzioni impartite in relazione ai dati personali trattati.

Trasferimento dei dati fuori dell'Unione Europea

Il Codice della privacy definisce regole precise per il trasferimento dei dati personali fuori dall'Unione europea e vieta, in linea di principio, il trasferimento "anche temporaneo" di dati personali verso uno Stato

extraeuropeo, qualora l'ordinamento del Paese di destinazione o di transito dei dati non assicuri un adeguato livello di tutela. Questa evenienza può verificarsi frequentemente nel caso in cui si decida di usufruire di servizi di *public cloud* invece che di modalità private o ibride. Per le sue valutazioni il titolare del trattamento (in genere chi acquista servizi cloud) dovrà quindi tenere in debito conto anche il luogo dove vengono conservati i dati e quali sono i trattamenti previsti all'estero.
Il trasferimento di dati verso gli Stati Uniti, ad esempio, può essere facilitato nel caso in cui il cloud provider aderisca a programmi di protezione dati come il cosiddetto *Safe Harbor* (letteralmente "porto sicuro"), un accordo bilaterale Ue-Usa che definisce regole sicure e condivise per il trasferimento dei dati personali effettuato verso aziende presenti sul territorio americano.

Le limitazioni per il trasferimento dati all'estero incidono anche sugli spostamenti "infragruppo" di una multinazionale.
In questo caso, la presenza di forti "norme vincolanti d'impresa" (*binding corporate rules*) a tutela dei dati personali può consentire l'eventuale trasferimento dei dati nel rispetto della privacy degli interessati.

Sicurezza dei dati
Il titolare del trattamento deve assicurarsi che siano adottate misure

tecniche e organizzative volte a ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, di modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole. Il cliente dovrebbe, ad esempio, accertarsi che i dati siano sempre "disponibili" (che si possa cioè sempre accedere ai dati) e "riservati" (che l'accesso cioè sia consentito solo a chi ne ha diritto). Per garantire che i dati siano al sicuro, non sono importanti solo le modalità con cui sono conservati, ma anche quelle con cui sono trasmessi (ad esempio utilizzando tecniche di cifratura).

I diritti dell'interessato

I soggetti pubblici e le imprese che decidono di avvalersi di servizi cloud per gestire i dati personali dei loro utenti o clienti non devono dimenticare che il Codice della privacy attribuisce agli interessati (le persone a cui si riferiscono i dati) precisi diritti. Ad esempio, l'interessato ha diritto di conoscere quali siano i dati che lo riguardano in possesso dell'amministrazione pubblica o dell'impresa, per quale motivo siano stati raccolti e come siano elaborati. Può richiedere una copia intelligibile dei dati personali che lo riguardano, il loro aggiornamento, la rettifica o l'integrazione. In caso di violazione di legge, può esigere anche il blocco, la cancellazione o la trasformazione in forma anonima di queste informazioni. Il cliente del servizio cloud, in qualità di titolare del trattamento dati, per soddisfare queste richieste, deve poter mantenere un adeguato controllo non solo sulle attività del fornitore, ma anche su quelle degli eventuali sub fornitori dei quali il cloud provider potrebbe avvalersi.


VALUTAZIONE DEI RISCHI,
DEI COSTI E DEI BENEFICI

È opportuno scegliere bene il tipo di cloud e il modello di servizio più adatto alle proprie esigenze. In particolare se si decide di adottare il *public cloud*, dove quasi tutto il processo viene esternalizzato e i "nostri" dati più preziosi sono dislocati "lontano" dal nostro controllo diretto. Il concetto di cloud può apparire evanescente, "virtuale".
In realtà, con le sue tecnologie si possono gestire servizi estremamente concreti, quali la distribuzione dei prodotti di un'azienda, i servizi dell'anagrafe di un Comune, le prenotazioni e le analisi mediche, il conto bancario on line e tanto altro. Nessuno lascerebbe in deposito il proprio portafoglio con i documenti e lo stipendio alla prima persona incontrata al mercato. Né affiderebbe il proprio libro mastro o i contratti stipulati con clienti e fornitori a un commercialista sconosciuto che gli promette di risparmiare, senza prima essersi accertato su come saranno conservati o utilizzati documenti così preziosi. La voce "risparmio" non deve quindi essere l'unico fattore di scelta.
I grandi fornitori globali di cloud computing si contano sulle dita di una mano. Quasi tutte le altre società che offrono servizi e infrastrutture tra le "nuvole" si avvalgono infatti delle aziende leader mondiali. Questa situazione riduce di molto la capacità negoziale di una singola impresa o di una piccola amministrazione pubblica, rendendo difficile trasformare la flessibilità tecnologica in flessibilità contrattuale.
In questi casi la scelta di consorziarsi con altri soggetti pubblici o imprese che hanno le medesime esigenze (ad esempio tramite le associazioni di categoria) potrebbe garantire una capacità contrattuale maggiore.
Prima di optare per un certo tipo di "nuvola", è comunque opportuno che l'utente verifichi la quantità e la tipologia

di dati che intende esternalizzare (ad esempio dati personali, in particolare quelli sensibili, oppure dati critici per la propria attività, come progetti riservati o coperti da brevetto o segreto industriale), valutando gli eventuali rischi e le possibili conseguenze derivanti da tale scelta. È vero che il cliente spesso non ha capacità di negoziare una riformulazione dei "*term of use*" proposti da chi offre i servizi: può però scegliere tra differenti provider. Anche i fornitori cloud, comunque, potrebbero trarre nuove opportunità dalla definizione di clausole "pro-privacy" o da una eventuale preventiva certificazione indipendente sul rispetto della normativa europea sulla protezione dei dati personali per i servizi da loro offerti. La risposta ad alcune domande può aiutare a sviluppare una corretta analisi dell'impatto economico e organizzativo di queste tecnologie all'interno di un'impresa o di una pubblica amministrazione.

SICUREZZA

Quali sono le misure di sicurezza adottate dal fornitore per proteggere i dati? Il fornitore di servizi cloud spesso dispone di sistemi di protezione contro virus, attacchi hacker o altri pericoli informatici più efficaci rispetto a quelli che potrebbe permettersi il singolo utente. È comunque necessario informarsi bene su quali siano le misure adottate dal cloud provider. Prima di scegliere il partner cloud il cliente deve sempre considerare che, affidandosi a un fornitore remoto, può perdere il controllo diretto ed esclusivo sui propri dati.

RUOLI E RESPONSABILITÀ

Chi è il reale fornitore del servizio che si sta acquisendo? Si tratta di una singola società o di un consorzio di imprese? Il servizio prescelto potrebbe essere il risultato finale di una "catena di

trasformazione" di servizi acquisiti presso altri service provider, diversi dal fornitore con cui l'utente stipula il contratto di servizio. L'utente, a fronte di filiere di responsabilità complesse, potrebbe non essere messo in grado di sapere chi, tra i vari gestori dei servizi intermedi, può accedere a determinati dati.

DISPONIBILITÀ DEL SERVIZIO E PIANO DI EMERGENZA

In caso di problemi al collegamento Internet, è comunque possibile continuare a usufruire dei servizi senza l'accesso al cloud? In quanto tempo può essere ripristinato il sistema? Esistono piani di emergenza per i servizi essenziali? Il servizio virtuale, in assenza di adeguate garanzie in merito alla qualità della connettività di rete, potrebbe occasionalmente risultare degradato in presenza di attacchi informatici, di elevati picchi di traffico o addirittura

indisponibile laddove si verifichino eventi anomali o guasti che impediscano l'accessibilità temporanea ai dati. È quindi necessario valutare bene le conseguenze sulla propria società o ente dell'eventuale interruzione, più o meno prolungata, del servizio, considerare i costi diretti e indiretti dell'inaccessibilità ai dati, e definire in anticipo con il fornitore cloud un eventuale piano di emergenza.

RECUPERO DEI DATI

È possibile che i dati sul cloud possano essere persi o distrutti? Calamità naturali o attacchi informatici potrebbero compromettere il funzionamento di alcuni data center. È particolarmente importante individuare possibili procedure di recupero dei dati

e quantificare l'impatto economico e organizzativo dell'eventuale perdita o cancellazione di dati presenti solo sul cloud.

CONFIDENZIALITÀ

Esistono garanzie di riservatezza per i nostri dati nel caso in cui un concorrente condivida gli stessi servizi cloud?
I fornitori custodiscono dati di singoli e di organizzazioni che potrebbero avere interessi ed esigenze differenti o persino obiettivi contrastanti e in concorrenza. È quindi opportuno valutare le garanzie offerte a tutela della confidenzialità delle informazioni trasferite sul cloud.

COLLOCAZIONE DEI SERVER

In quale Stato sono conservati i dati caricati sulla "nuvola"? È possibile scegliere di usufruire di server collocati solo in territorio nazionale o in Paesi dell'Unione europea? L'identificazione del luogo in cui i dati sono conservati o elaborati ha riflessi immediati sia sulla normativa applicabile in caso di contenzioso tra il cliente e il fornitore, sia in relazione alle disposizioni nazionali che disciplinano il trattamento, l'archiviazione e la sicurezza dei dati.
La conoscenza di questi elementi garantirà un rapporto più trasparente tra il cliente e il fornitore di cloud computing. È poi necessario non dimenticare che la normativa sulla privacy, al fine di tutelare le persone interessate, prevede che i dati possano essere "esportati" in Paesi fuori dall'Unione europea solo in precisi casi e quando sia offerta una protezione adeguata rispetto a quella prevista dalla legislazione comunitaria. Un servizio cloud potrebbe quindi celare dei costi extra imprevisti, determinati dalla ridotta capacità di controllo sui propri dati o da più probabili contenziosi legali nazionali e internazionali.

MIGRAZIONE

La tecnologia utilizzata dal fornitore di cloud è di tipo "proprietario"? I dati possono essere esportati facilmente? L'adozione da parte del fornitore del servizio di tecnologie proprie può, in taluni casi, rendere complessa per l'utente la migrazione di dati e documenti da un sistema cloud ad un altro o lo scambio di informazioni con soggetti che utilizzino servizi cloud di fornitori differenti, ponendo quindi a rischio la portabilità o l'interoperabilità dei dati. Questa evenienza potrebbe dare luogo a politiche commerciali poco trasparenti. In un primo momento, il fornitore potrebbe ad esempio presentare al cliente un'offerta di servizi cloud economicamente vantaggiosa e con adeguate garanzie a protezione dei dati. In un secondo momento, una volta acquisito il cliente, potrebbe invece cambiare le condizioni del contratto a proprio vantaggio con la certezza che il cliente - considerata l'impossibilità pratica di trasferire agevolmente i dati presso un altro fornitore e di recedere dal servizio - non potrà far altro che accettarle.

ASSICURAZIONE SUL DANNO

Nel caso in cui si accerti una violazione o la perdita dei dati, il fornitore garantisce un pronto risarcimento del danno? Le attuali incertezze normative possono rendere difficile e oneroso riuscire a ottenere un adeguato risarcimento per i danni subiti in seguito a violazioni, a perdita di dati, a interruzione anche temporanea del servizio cloud.
La presenza di un'assicurazione o di procedure semplificate per la risoluzione di controversie, anche internazionali, può sicuramente essere un valore aggiunto per utenti di piccole dimensioni.


IL DECALOGO
PER UNA SCELTA
CONSAPEVOLE
1
2
3

1

EFFETTUARE UNA VERIFICA SULL'AFFIDABILITÀ DEL FORNITORE

Gli utenti dovrebbero accertare l'esperienza, la capacità e l'affidabilità del fornitore prima di trasferire sui sistemi cloud i propri dati più preziosi, tenendo in considerazione le proprie esigenze istituzionali o imprenditoriali, la quantità e la tipologia delle informazioni che intendono allocare, i rischi e le misure di sicurezza adottate. Anche in funzione della tipologia di servizio desiderato, oltre che della criticità dei dati, è opportuno che gli utenti valutino: la struttura societaria del fornitore, le referenze, le garanzie di legge offerte in ordine alla confidenzialità dei dati e alle misure adottate per assicurare la continuità operativa a fronte di eventuali e imprevisti malfunzionamenti.
Gli utenti dovrebbero valutare, inoltre, le caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità.
Sarà utile considerare anche l'impiego da parte del fornitore di personale qualificato, l'adeguatezza delle sue infrastrutture informatiche e di comunicazione, la disponibilità ad assumersi una responsabilità risarcitoria (che dovrebbe essere esplicitamente prevista dal contratto di servizio) in caso di eventuali falle nel sistema di sicurezza o di interruzioni del servizio.

2

PRIVILEGIARE I SERVIZI CHE FAVORISCONO LA PORTABILITÀ DEI DATI

È consigliabile ricorrere a servizi di cloud computing privilegiando quelli basati su formati e standard aperti, che facilitino la transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi.

La portabilità dei dati consente di recedere dal servizio senza incorrere in spese e disagi difficilmente prevedibili. Tale opzione limita anche il rischio che i fornitori, sfruttando la loro posizione di forza negoziale, adottino eventuali modifiche unilaterali e peggiorative dei contratti di servizio cloud instaurati con il cliente.

3

ASSICURARSI LA DISPONIBILITÀ DEI DATI IN CASO DI NECESSITÀ

È opportuno chiedere che nel contratto con il fornitore siano ben specificate adeguate garanzie sulla disponibilità e sulle prestazioni dei servizi cloud. L'adozione di servizi che non offrono adeguate garanzie di riservatezza e di continuità operativa può comportare rilevanti ripercussioni non solo sul cliente del servizio cloud, ma anche sui soggetti a cui si riferiscono i dati personali trattati, come avviene per le pubbliche amministrazioni e per le società che offrono servizi a terzi. In tal senso, a fronte del contenimento dei costi, il titolare del trattamento (in genere chi acquista servizi cloud) dovrà comunque prevedere la possibilità di conservare una copia dei dati allocati sul cloud, in particolare di quelli la cui perdita o indisponibilità potrebbe causare gravissimi danni, non solo economici o di immagine: si pensi a dati particolarmente delicati come quelli di tipo sanitario o giudiziario, o di carattere fiscale e patrimoniale.

4

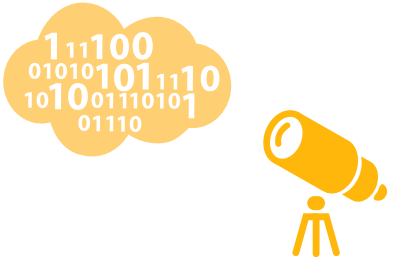
SELEZIONARE I DATI DA INSERIRE NELLA NUVOLA

Alcune informazioni, come quelle coperte da segreto industriale e tutti i dati sensibili (ad esempio quelli relativi alla salute, all'etnia, alle opinioni politiche o alle iscrizioni a sindacati), richiedono, per loro intrinseca natura, particolari misure di sicurezza.
In tali casi, poiché dall'inserimento dei dati nel cloud consegue comunque una inferiore capacità di controllo diretto da parte dell'utente e un'esposizione a rischi non sempre prevedibili di perdita o di accesso abusivo, è bene valutare con responsabile attenzione se ricorrere ai servizi di cloud computing (in particolare di tipo "pubblico"), oppure se utilizzare altre forme di *outsourcing*, ovvero mantenere "in sede" il trattamento di tali dati.

5

NON PERDERE DI VISTA I DATI

È sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto, anche verificando se i dati rimarranno nella disponibilità fisica dell'operatore con cui è stato stipulato il contratto oppure se questi svolga un ruolo di intermediario, ovvero offra un servizio basato sulle tecnologie messe a disposizione da un operatore terzo.
Si pensi, ad esempio, a un applicativo in modalità cloud nel quale il fornitore



del servizio finale di elaborazione dati si avvalga di un servizio di "stoccaggio" acquisito da un terzo. In tal caso, saranno i sistemi fisici di quest'ultimo operatore che concretamente ospiteranno i dati immessi nel cloud dall'utente. Per valutare la qualità del cloud è quindi necessario informarsi sulle prestazioni offerte da tutti i soggetti coinvolti nella fornitura del servizio.

6

INFORMARSI SU DOVE RISIEDERANNO, CONCRETAMENTE, I DATI

È importante per l'utente sapere se i propri dati vengono trasferiti ed elaborati da server in Italia, in Europa o in un Paese extraeuropeo. Tale informazione può essere determinante per stabilire la giurisdizione e la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio, ma soprattutto per verificare il livello di protezione assicurato ai dati.
Il trasferimento di dati in Paesi che non offrono adeguate garanzie di sicurezza e confidenzialità potrebbe comportare un illecito trattamento dei dati personali, oltre a eventuali danni irreparabili per le attività istituzionali dei soggetti pubblici o per il business delle imprese.
In ogni caso, l'utente, prima di caricare i dati "sulla nuvola" e di consentire il loro eventuale trasferimento in Paesi fuori dall'Unione europea, deve accertarsi che questo spostamento avvenga nel rispetto delle garanzie previste dalla normativa italiana e comunitaria in tema di protezione dei dati personali.
Se l'azienda, ad esempio, è statunitense è bene verificare che abbia aderito all'accordo *Safe Harbor* che definisce regole condivise con le istituzioni europee per il trattamento dei dati personali.
Così come è utile controllare che

le aziende al di fuori dell'Ue coinvolte nel cloud abbiano sottoposto le proprie procedure di sicurezza e di trattamento dei dati a specifici percorsi di certificazione, come quelli regolati dagli standard ISO per la gestione della sicurezza. Oppure se nei contratti di *outsourcing* proposti al cliente siano state inserite le specifiche "clausole contrattuali tipo" approvate dalla Commissione europea per i trasferimenti di dati personali verso Paesi terzi.

7

ATTENZIONE ALLE CLAUSOLE CONTRATTUALI

È importante valutare l'idoneità delle condizioni contrattuali per l'erogazione del servizio di cloud con particolare riferimento agli obblighi e alle responsabilità in caso di perdita e di illecita diffusione dei dati custoditi nella "nuvola", nonché alle eventuali modalità per il recesso dal servizio e il passaggio ad altro fornitore.
Un elemento da privilegiare è senz'altro la previsione di garanzie di qualità chiare, corredate da penali, che pongano a carico del fornitore le eventuali inadempienze o le conseguenze di determinati eventi (ad es. accesso non consentito, perdita dei dati, indisponibilità per malfunzionamenti ecc.).
Si suggerisce di verificare anche l'eventuale partecipazione di ulteriori soggetti che concorrano come subfornitori all'erogazione del servizio cloud e all'eventuale trattamento dei dati.

8

VERIFICARE TEMPI E MODALITÀ DI CONSERVAZIONE DEI DATI

In fase di acquisizione del servizio cloud è opportuno approfondire e prevedere nel contratto le politiche adottate dal fornitore riguardo ai tempi

di conservazione dei dati nella nuvola. Ove non sia già prevista per legge l'immediata cancellazione dei dati del titolare allo scadere del contratto cloud, è necessario accertare il termine ultimo oltre il quale il fornitore (responsabile del trattamento) debba cancellare definitivamente i dati a lui affidati. Il fornitore dovrà quindi assicurare che i dati non saranno conservati oltre i suddetti termini o comunque al di fuori di quanto esplicitamente stabilito con l'utente stesso. In ogni caso, i dati dovranno essere sempre conservati solo nel rispetto delle finalità e delle modalità concordate.

9

ESIGERE ADEGUATE MISURE DI SICUREZZA

Nell'ottica di proteggere la confidenzialità dei dati, occorre valutare con attenzione anche le misure di sicurezza utilizzate dal fornitore del servizio cloud. In generale si raccomanda di privilegiare i fornitori che utilizzino modalità di archiviazione e trasmissione sicure, mediante tecniche crittografiche (specialmente quando i dati trattati sono particolarmente delicati), accompagnate da robusti meccanismi di identificazione dei soggetti autorizzati all'accesso.

10

FORMARE ADEGUATAMENTE IL PERSONALE

Il personale, sia quello del cliente che quello del fornitore, incaricato del trattamento dei dati mediante servizi di cloud computing dovrebbe essere

appositamente formato, al fine di limitare rischi di accesso illecito, di perdita di dati o, più in generale, di trattamento non consentito. L'attività di formazione dovrebbe riguardare sia gli elementi tecnici che consentono una scelta consapevole delle tecnologie cloud adottate, sia le fasi operative del trattamento, come l'inserimento dei dati sulla "nuvola" e la loro elaborazione. La protezione dei dati può infatti essere messa a repentaglio non solo da eventuali comportamenti sleali o fraudolenti, ma anche da errori materiali, leggerezza o negligenza del personale.

UNA PRECAUZIONE EXTRA PER GLI UTENTI PRIVATI

Le disposizioni previste dal Codice della privacy non si applicano a singole persone che trattano i dati per scopi personali, senza diffonderli magari su Internet e senza effettuare comunicazioni sistematiche di tali dati a più individui. È comunque opportuno ricordare che anche le cosiddette "persone fisiche" sono tenute a conservare con cura i dati affinché la loro eventuale perdita non possa causare danni ad altre persone. L'adozione di nuove tecnologie per la mobilità, come smartphone e tablet, dotati di grandi quantità di memoria, spesso connessi a servizi cloud non protetti che consentono di sfruttare lo stesso strumento per attività private e professionali, ha però aumentato il rischio di perdita di controllo dei dati personali. Si consiglia quindi di conservare con cura gli strumenti tecnologici utilizzati per scopi personali, e di adottare tutte le cautele al fine di impedire accessi anche accidentali, da parte di terzi, ai dati personali.

LA PRIVACY A SCUOLA

DAI TABLET ALLA PAGELLA ELETTRONICA LE REGOLE DA RICORDARE


Temi in classe
Cellulari e tablet
Recite e gite scolastiche
Rette e servizio mensa
Videosorveglianza
Inserimento professionale
Questionari per attività di ricerca
Iscrizioni e registri on line, pagella elettronica
Voti, scrutini, esami di Stato
Trattamento dei dati personali

Temi in classe

Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale.

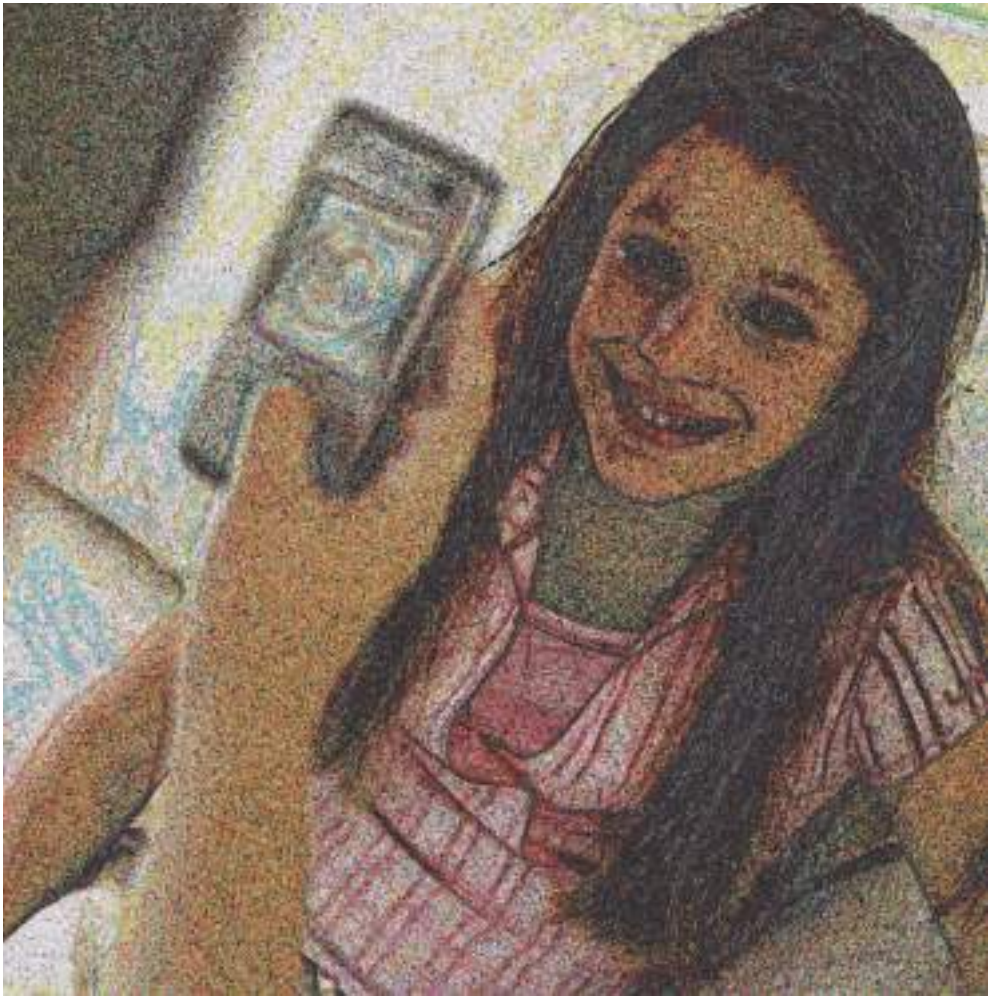
Sta invece nella sensibilità dell'insegnante, nel momento in cui gli elaborati vengono letti in classe, trovare l'equilibrio tra esigenze didattiche e tutela della riservatezza, specialmente se si tratta di argomenti delicati.

Cellulari e tablet

L'uso di cellulari e smartphone è in genere consentito per fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone.

Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. E' bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati.

Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line.



Recite e gite scolastiche

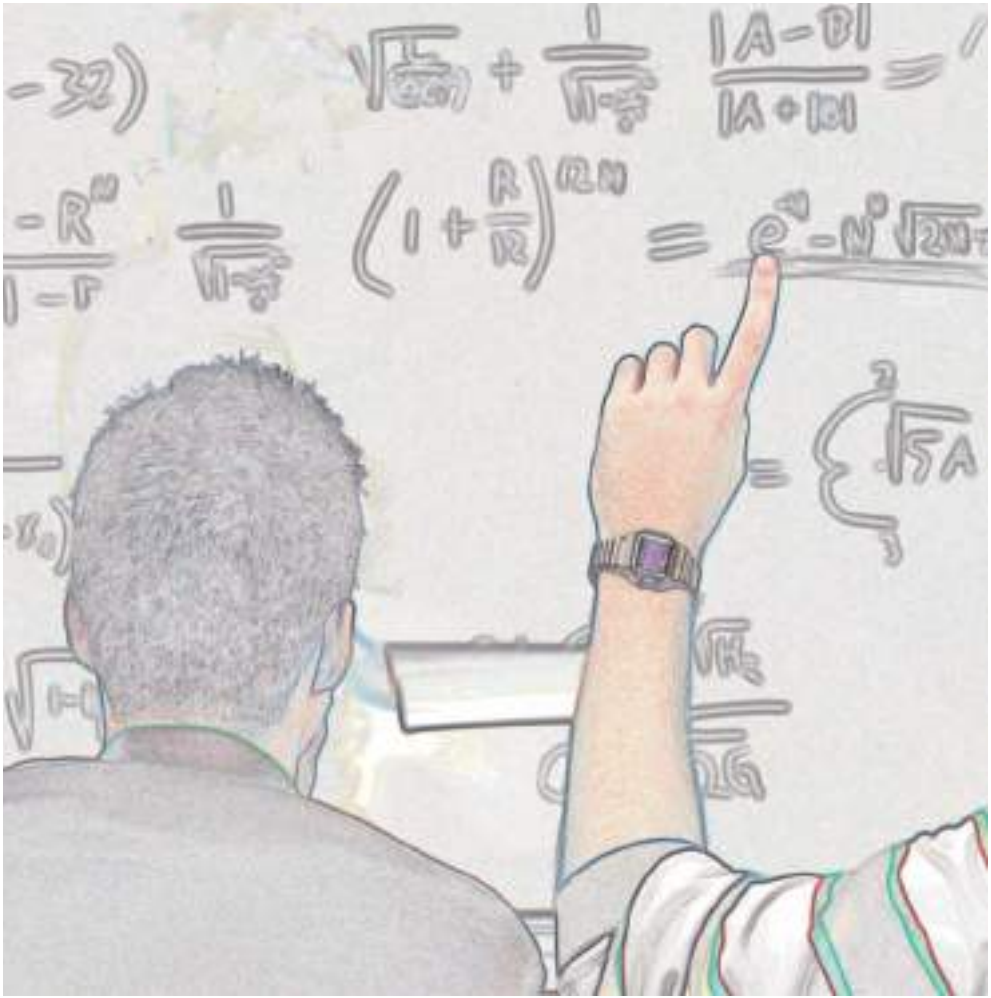
Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini in questi casi sono raccolte a fini personali e destinati ad un ambito familiare o amicale. Nel caso si intendesse pubblicarle e diffonderle in rete, anche sui social network, è necessario ottenere di regola il consenso delle persone presenti nei video o nelle foto.

Retta e servizio mensa

E' illecito pubblicare sul sito della scuola il nome e cognome degli studenti i cui genitori sono in ritardo nel pagamento della retta o del servizio mensa.
Lo stesso vale per gli studenti che usufruiscono gratuitamente del servizio mensa in quanto appartenenti a famiglie con reddito minimo o a fasce deboli.
Gli avvisi messi on line devono avere carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale.
A salvaguardia della trasparenza sulla gestione delle risorse scolastiche, restano ferme le regole sull'accesso ai documenti amministrativi da parte delle persone interessate.

Telecamere

Si possono in generale installare telecamere all'interno degli istituti scolastici, ma devono funzionare solo negli orari di chiusura degli istituti e la loro presenza deve essere segnalata con cartelli. Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere deve essere opportunamente delimitato. Le immagini registrare devono essere cancellate in generale dopo 24 ore.



Inserimento professionale

Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale le scuole, su richiesta degli studenti, possono comunicare e diffondere alle aziende private e alle pubbliche amministrazioni i dati personali dei ragazzi.

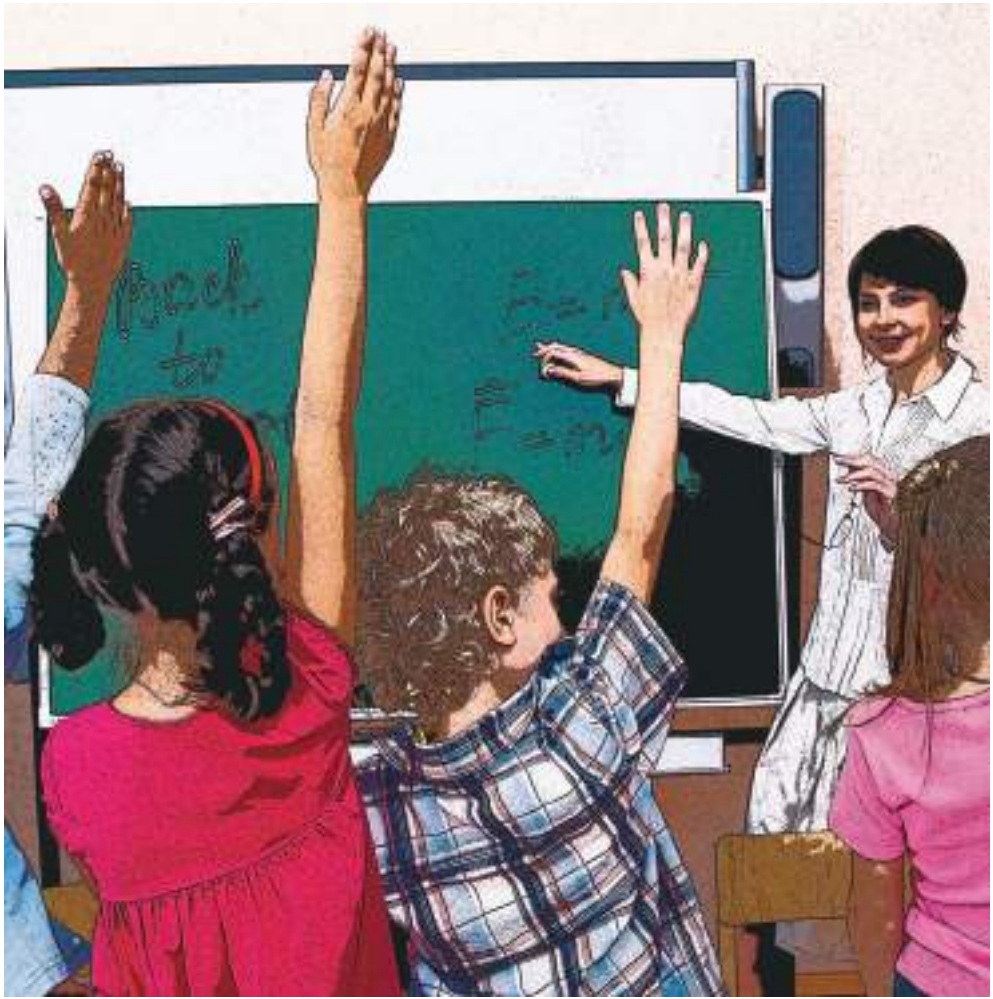
Questionari per attività di ricerca

L'attività di ricerca con la raccolta di informazioni personali tramite questionari da sottoporre agli studenti è consentita solo se ragazzi e genitori sono stati prima informati sugli scopi delle ricerca, le modalità del trattamento e le misure di sicurezza adottate.

Gli studenti e i genitori devono essere lasciati liberi di non aderire all'iniziativa.

Iscrizione e registri on line, pagella elettronica

In attesa di poter esprimere il previsto parere sui provvedimenti attuativi del Ministero dell'istruzione riguardo all'iscrizione on line degli studenti, all'adozione dei registri on line e alla consultazione della pagella via web, il Garante auspica l'adozione di adeguate misure di sicurezza a protezione dei dati.



Voti, scrutini, esami di Stato

I voti dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato sono pubblici. Le informazioni sul rendimento scolastico sono soggette ad un regime di trasparenza e il regime della loro conoscibilità è stabilito dal Ministero dell'istruzione.

E' necessario però, nel pubblicare voti degli scrutini e degli esami nei tabelloni, che l'istituto eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti: il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap, ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.

Trattamento dei dati personali

Le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano.
Spesso le scuole utilizzano nella loro attività quotidiana dati delicati - come quelli riguardanti le origini etniche, le convinzioni religiose, lo stato di salute - anche per fornire semplici servizi, come ad esempio la mensa.

E' bene ricordare che nel trattare queste categorie di informazioni gli istituti scolastici devono porre estrema cautela, in conformità al regolamento sui dati sensibili adottato dal Ministero dell'istruzione.
Famiglie e studenti hanno diritto di conoscere quali informazioni sono trattate dall'istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

CONNETTILATESTA!

"Quando ti connetti ai social network, connetti anche la testa"!

Con i **social network** entri in contatto con gli altri, condividi idee ed emozioni, cerchi e trovi informazioni.

Queste nuove forme di comunicazione offrono enormi opportunità, ma presentano anche dei rischi che è bene conoscere.

Per aiutarti, il **Garante per la protezione dei dati personali** mette a tua disposizione tre strumenti: un **video tutorial** per riflettere su come usare i social network in modo sicuro e consapevole, un breve **questionario** per testare quanto conosci i principali pericoli che si possono correre in Rete e un **vademecum** con i consigli dell'Autorità.

Il video tutorial
“Quando ti connetti ad un social network, connetti anche la testa!”

Quando ti connetti ad un social network, connetti anche la testa!

(Il testo del video)

Che bello usare il web per comunicare, cercare informazioni, postare idee ed emozioni, attraverso parole, musica, foto e filmati. Con i social network ci divertiamo, costruiamo legami ed amicizie, riceviamo notizie dal mondo. E possiamo perfino usarli per studiare e lavorare. Un mondo intero, che oggi è sempre letteralmente a portata di mano grazie a smartphone e tablet.
Un mondo che però può presentare anche qualche rischio.

Intanto, cerca di ricordarti che tutto quello che pubblichi probabilmente rimarrà lì per sempre e che puoi anche perderne il controllo. Oggi magari sei contento che tutti possano leggere i tuoi pensieri o vedere le tue foto… ma domani?

Prima di mettere online qualcosa, quindi, fatti qualche domanda. Tipo:

- vuoi davvero che tutti sappiano certe cose di te? Cosa fai, cosa pensi, dove vai e con chi… Condividere certe informazioni è un'arma a doppio taglio. Ad esempio, è divertente scrivere che a una festa hai bevuto un po' troppa birra con gli amici e postare magari anche una foto o un video. Ma cosa potrebbero pensare i tuoi genitori, i tuoi professori o addirittura chi domani ti farà un colloquio di lavoro?
- E poi: le cose che pubblichi possono offendere qualcuno? Sei sicuro che i tuoi amici siano contenti di vedere online foto in cui ci sono anche loro o che certe battute piacciano davvero a tutti?

C'è un altro aspetto importante. Hai mai sentito parlare di ladri di identità? Persone che girano in Internet per rubare i tuoi dati personali, e usarli poi per tempestarti di messaggi o addirittura per compiere reati.

Quando navighi, quindi, segui alcune regole per proteggerti dai malintenzionati.

In primo luogo, stai attento a non comunicare a sconosciuti alcune informazioni molto personali come il tuo indirizzo, il numero di cellulare o il numero di carta di credito, se ne hai una.

E poi: non accettare amicizie a caso. Avere molti contatti sui social network è bello, ma non puoi mai sapere con chi hai a che fare e se per caso ha cattive intenzioni.
Infine, conserva solo per te la password di accesso ai social network, e ricorda di cambiarla ogni tanto. E cerca di usare password diverse per accedere a siti diversi e alla posta elettronica. Perché altrimenti, rubata una password, rubate tutte!

La miglior difesa è informarsi. In ogni social network c'è una pagina che spiega come vengono gestite le notizie che ti riguardano: cerca di leggerla, anche se può sembrarti un pò noiosa. Scoprirai cose molto importanti.
Cerca anche di capire come fare per proteggere la tua riservatezza, controllando le tue impostazioni privacy. Se vuoi andare sul sicuro, in pochi click puoi decidere che certe informazioni possono vederle solo i tuoi amici e non anche dei perfetti sconosciuti.
E se ti dà fastidio essere bombardato di messaggi pubblicitari, quando ti iscrivi a un social network fai attenzione alle condizioni d'uso del servizio. Ad esempio, verifica se puoi impedire che i tuoi dati personali possano essere usati per inviarti pubblicità indesiderata.

Se hai bisogno di aiuto per proteggere la tua privacy o per avere informazioni utili per navigare in sicurezza, puoi rivolgerti al Garante per la protezione dei dati personali.

Ma ricorda sempre: il miglior garante della tua privacy online sei tu!

Il questionario del Garante per testare la conoscenza dei pericoli in Rete

Il vademecum con i consigli dell'Autorità

"FATTI SMART!"

Il video tutorial “Fatti Smart!”

Le indicazioni del Garante per tutelare la tua privacy quando usi smartphone e tablet

Non ci pensiamo quasi mai, forse. Smartphone e tablet ci accompagnano ovunque e custodiscono parti importanti e spesso delicate delle nostre vite, sotto forma di foto, filmati, messaggi e dati telematici. E noi stiamo sempre attenti a proteggere adeguatamente queste informazioni con piccole ma utili precauzioni?

In un **video-tutoria**l il Garante per la protezione dei dati personali offre alcune utili indicazioni per tutelare la nostra privacy quando utilizziamo smartphone e tablet.

Attenzione ai dati conservati su smartphone e tablet
Non conservare su smartphone e tablet informazioni troppo personali che potrebbero essere smarrite o rubate, o perfino clonate o attaccate da pirati elettronici. Non si dovrebbero mai conservare, ad esempio, password personali, codici di accesso e dati bancari in chiaro.
Ricorda, poi, che smartphone e tablet venduti, regalati o buttati possono contenere ancora dati privati. Se te ne liberi, quindi, cerca di adottare alcune piccole precauzioni di sicurezza come:

- ripristinare le impostazioni di fabbrica
- rimuovere la scheda SIM e la scheda di memoria
- eliminare tutti i backup contenuti nella memoria.

Proteggi i tuoi dati
Se vuoi evitare che qualcuno legga di nascosto le tue e-mail e i tuoi sms o che usi a tua insaputa il tuo smartphone o il tuo tablet, usa alcune precauzioni.

Imposta sempre un codice PIN abbastanza complicato, evitando, ad esempio, di usare il tuo nome e cognome, la data di nascita, il nome dei figli o quello del gatto di casa, o comunque altre parole che ti renderebbero in qualche modo riconoscibile.
Magari imposta anche un codice di blocco, quello che si attiva automaticamente quando il cellulare è acceso ma non viene utilizzato per un po' di tempo. E anche in questo caso, evita codici un po' troppo facili da scoprire.
Alcuni sistemi operativi consentono anche di impostare password di sicurezza che bloccano completamente l'accesso ai dati personali. Per farlo, basta collegare smartphone e tablet con il pc e utilizzare il software per la gestione del prodotto.
Conserva con cura il codice IMEI, che trovi sulla scatola del prodotto che acquisti e che in caso di furto o smarrimento puoi utilizzare per bloccare a distanza l'accesso al tuo smartphone o tablet.

Quando navighi su smarthone e tablet
Se ti connetti a Internet e ai social network via smartphone e tablet, verifica le impostazioni privacy e leggi le condizioni d'uso dei servizi.
Per navigare sul web, inoltre, installa sempre - se disponibile - software di sicurezza anti-virus informatici o contro le intrusioni da parte di pirati telematici e ladri d'identità digitali.
Quando usi connessioni wi-fi gratuite, ad esempio nei locali pubblici, verifica che la navigazione sia protetta con protocolli di scambio dati criptati e che l'autenticazione ai siti che eventualmente vengono visitati utilizzi il protocollo HTTPS. In caso contrario, se si utilizzano credenziali di accesso a siti e servizi come la posta elettronica o l'home banking, il rischio che non ci siano adeguate garanzie di sicurezza per i propri dati è reale.

APP-rova di privacy

Se scarichi delle applicazioni, evita le fonti sconosciute e utilizza sempre i market ufficiali, a meno che tu non sia in grado di valutare autonomamente l'affidabilità della fonte - ad esempio leggendo i commenti eventualmente lasciati dagli altri utenti - per comprendere se ci sono eventuali rischi o problematiche.

Una volta installata un'applicazione, verifica se richiede l'accesso a contenuti presenti sul tuo smartphone o sul tuo tablet (ad esempio, le tuo foto o i contatti in rubrica) e leggi con attenzione le condizioni d'uso del servizio, soprattutto per evitare di dover pagare servizi non richiesti o di vedere esposte oltremisura informazioni di carattere personale (ad esempio: foto, video, contatti, ecc.).

Occhio allo spam

Smartphone e tablet sono terreno di caccia per lo spam.

Attenzione ai link presenti in e-mail, sms e messaggistica istantanea, perché, in alcuni casi, cliccandoli, potresti inconsapevolmente accettare di ricevere comunicazioni indesiderate, divenendo bersaglio di messaggi pubblicitari non richiesti da cui, poi, può anche essere abbastanza difficile liberarsi.

Vuoi sempre far sapere dove sei?

Smartphone e tablet hanno funzioni di geolocalizzazione, ma sei tu a decidere se, quando e chi può conoscere la tua posizione.

Per disabilitare la geolocalizzazione, puoi disattivare - controllando le impostazioni dello smartphone o tablet - il GPS o la connessione wi-fi quando non usi questi servizi o altri ad essi collegati.

E' bene, inoltre, controllare anche le impostazioni di geolocalizzazione dei servizi di social network che eventualmente utilizzi su smartphone o tablet. La scelta finale di far sapere o meno dove sei, in fin dei conti, è sempre la tua.

PROBLEMI DI SPAM????

Il video tutorial
“Problemi di spam????”

Il vademecum
“Spam: come difendersi.
Le indicazioni del Garante privacy”

Spam: come difendersi. Le indicazioni del Garante privacy

Spamming o **spam** è l'invio, talora massiccio e ripetuto, tramite operatore o con modalità automatizzate, di **comunicazioni non richieste** (via telefono, e-mail, fax, sms o mms), senza che il destinatario abbia ricevuto un'**informativa** sul trattamento dei dati personali o abbia prestato il consenso a ricevere messaggi. Negli ultimi tempi, lo spamming sta interessando anche il mondo dei social network e quello dei sistemi di messaggistica per smartphone e tablet.
Lo **spammer** - cioè colui che invia lo spam - utilizza riferimenti (e-mail, numeri telefonici, ecc.) per l'invio di messaggi promozionali spesso raccolti in modo non lecito o in maniera automatica via Internet (su gruppi *Usenet*, *newsgroups*, *forum*, ecc.), mediante speciali programmi (*spambot*, ecc.) o, più semplicemente, facendo invii massivi a caso ad indirizzi e-mail basati sull'uso di nomi comuni Scopo dello spamming è veicolare messaggi pubblicitari, ma tale pratica è legata anche a veri e propri tentativi di truffa, come il *phishing*. In Italia l'invio di messaggi automatizzati a fini promozionali non desiderati è soggetto a sanzioni amministrative e penali.

Come prevenire lo spam?
- **Non diffondere**, soprattutto on-line, il tuo indirizzo e-mail o il numero di telefono fisso o mobile;
- Se per ottenere un dato servizio (iscrizione a newsletter, acquisti on-line, ecc.) devi firmare un documento o iscriverti ad un sito web, **leggi sempre con attenzione le regole privacy e le condizioni d'uso del servizio**, e soprattutto verifica le modalità e le finalità del trattamento dei tuoi dati personali.
- Prendi in considerazione di **utilizzare più indirizzi e-mail** per le tue varie esigenze. Ad esempio, potresti crearne uno ad uso **esclusivamente** "commerciale", da impiegare per fare acquisti on-line, accedere a servizi su Internet, iscriverti a newsletter, ecc.. In questo modo, il rischio di "contagio spam" non coinvolgerebbe gli indirizzi di posta elettronica che utilizzi invece per le tue esigenze quotidiane più importanti (lavoro, amicizia, ecc.).

- Se hai un sito personale o un blog su cui vuoi pubblicare la tua e-mail, proteggila con accorgimenti che rendono la vita più difficile ai programmi (i cosiddetti *spider*) capaci di raccogliere in automatico gli indirizzi di posta elettronica per finalità di spamming.
- Se invii una e-mail a molti destinatari, **non rendere visibili gli indirizzi dei tuoi contatti** e usa la funzione "destinatario in copia conoscenza nascosta (*ccn*)". Stessa precauzione se frequenti dei newsgroups, dove possono essere attivi dei programmi *spider*.
- Prova ad usare i **filtri anti-spam** offerti, ad esempio, da alcuni programmi di posta elettronica, che possono aiutarti a bloccare tutti i messaggi provenienti da un particolare indirizzo. Tali funzioni possono essere disponibili anche per i social network e i servizi di messaggistica per smartphone e tablet.
- **Mantieni in efficienza il tuo pc**, scaricando periodicamente gli aggiornamenti (che contengono anche difese anti-spam) per il sistema operativo e gli applicativi più utilizzati, e installa eventualmente un programma anti-virus che offra anche una protezione anti-spam.
- **Se utilizzi i social network**:
  - controlla le impostazioni privacy del tuo account eventualmente limitando la visibilità del tuo profilo;
  - se disponibile, utilizza la funzione "di blocco" per i soggetti che inviano messaggi indesiderati;
  - non dare l'amicizia a soggetti sconosciuti;
  - evita di rendere pubblici sulla tua pagina personale il tuo indirizzo e-mail o il numero di cellulare.

Cosa non devi fare

- **Non rispondere allo spam**: la risposta può consentire allo spammer di stabilire che il tuo indirizzo e-mail è valido e attivo. Così può continuare a "spammarti" o rivendere il tuo indirizzo verificato a terzi. Può anche tentare di utilizzare il contatto creato per portare avanti tentativi di truffa.
- **Non cliccare su eventuali link** per la cancellazione dell'invio e tantomeno non fornire i tuoi dati personali senza aver prima fatto delle verifiche. Questi link potrebbero essere collegati a sistemi che consentono truffe telematiche e furti di identità, ma potrebbero anche aprire la strada a

software spia o a virus informatici. Per la stessa ragione, **non devi mai cliccare su collegamenti ipertestuali** inseriti nel corpo del testo o **aprire ed eseguire eventuali allegati**, soprattutto se contengono estensioni tipo ".exe". Se non sei sicuro del mittente, evita di scaricare le immagini eventualmente contenute nel corpo del messaggio e-mail.

Differenze tra spam e invii leciti

- Se il contatto e-mail o telefonico è stato **raccolto** con il consenso del destinatario o secondo le modalità previste dalla legge (es: nell'ambito di un contratto per la fornitura di un qualche servizio), non si può parlare di spam.
- In ogni caso, **se le comunicazioni pubblicitarie o altro tipo richieste** (es: invio di newsletter, ecc.) **risultano ad un certo punto indesiderate**, è tuo diritto opporti al trattamento dei tuoi dati inviando una e-mail al mittente per chiedere la sospensione dell'invio o utilizzando, se disponibili, le procedure on-line per la cancellazione dei tuoi dati dal database di chi ti invia le comunicazioni.

Come agire contro lo spam?

- **Se sei una persona fisica puoi**:
  - presentare segnalazioni, reclami e ricorsi al Garante per la protezione dei dati personali;
  - rivolgerti al giudice ordinario per l'eventuale risarcimento del danno.

- **Se sei una persona giuridica**:
  - puoi rivolgerti al giudice ordinario per il risarcimento del danno;
  - non puoi fare segnalazioni, reclami e ricorsi al Garante, che può però intervenire d'ufficio.

PRIVACY SOTTO L'ALBERO

Consigli per navigare sicuri durante le feste natalizie

1. Uso intelligente dei social network. Se durante le feste di Natale si parte per le vacanze, bisogna fare attenzione a non comunicare sul web per quanto tempo non si sarà in casa e in quali giorni. In ogni caso, è sempre bene evitare di postare informazioni riguardanti l'indirizzo di casa, il posto dove si parcheggia di solito o la targa dell'auto. I malintenzionati sono sempre in agguato…

2. Occhio agli Sms con auguri e offerte di Natale. Nell'epoca degli smartphone, i messaggi Sms possono contenere anche virus, link a servizi indesiderati a pagamento e programmi potenzialmente dannosi per la privacy. E' buona regola limitare la diffusione del proprio numero telefonico e non rispondere a messaggi provenienti da numeri sconosciuti.

3. Cartoline di auguri elettroniche. Fa piacere riceverle e spedirle via e-mail, Sms, Mms e social network. Ma possono contenere virus, malware (cioè programmi dannosi) o esporre al rischio di spam. E' sempre bene fare molta attenzione prima di scaricare programmi, aprire eventuali allegati o cliccare link contenuti nel testo o nelle immagini. Si possono poi adottare semplici precauzioni: ad esempio, non rispondere alle e-mail provenienti da sconosciuti, oppure passare il mouse su un link senza cliccarlo e verificare - in basso a sinistra nel browser - la Url (cioè, l'indirizzo web) reale al quale si potrebbe essere indirizzati.

4. Truffe e posta elettronica. Diffidare delle offerte di sconti straordinari su viaggi e regali da ottenere compiendo determinate operazioni (ad esempio, cliccare su link, fornire dati personali o bancari, ecc.), che possono arrivare via social network, e-mail o Sms. Malware, virus informatici, software spia e phishing (cioè, una frode finalizzata all'acquisizione, per scopi illegali, di dati riser-

vati dell'utente) possono essere in agguato. Anche qui, valgono le stesse precauzioni indicate per le cartoline elettroniche. Un pericolo in crescita nel periodo delle feste è quello delle false notifiche di spedizione, che avvisano dell'aggiornamento di un ordine mai effettuato o della necessità di ritirare un pacco. Nei casi dubbi, quando non si è effettuato alcun ordine e non si attende alcuna consegna, è bene evitare di fornire dati personali online, e non cliccare link sospetti o installare eventuali software indicati come necessari per completare le operazioni di spedizione e consegna. Le aziende del settore, infatti, operano abitualmente tramite altri canali.

5. Attenzione alle app. Durante le feste molti utenti di smartphone e tablet scaricano app gratuite per avere accesso a promozioni o negozi online, per creare e inviare cartoline di Natale o attivare giochi. Questi prodotti software possono anche nascondere virus o malware. Per proteggersi, buone regole sono: scaricare le app dai market ufficiali; leggere con attenzione le descrizioni dei programmi; consultare eventuali recensioni degli utenti; evitare che i minori possano scaricare le app da soli.

6. Falsi siti. Diffidare dello shopping online troppo scontato se non si è sicuri dell'affidabilità del sito, se l'indirizzo Internet del sito appare anomalo (ad esempio, se non corrisponde al nome dell'azienda che dovrebbe gestirlo) e se non vengono rispettate le procedure di sicurezza standard per le transazioni online (protocolli https). In ogni caso, è sempre bene fare estrema attenzione quando vengono richieste le credenziali della carta di credito o del conto bancario.

7. In vacanza, Wi-Fi gratuito ma con prudenza. Le connessioni offerte da locali e hotel potrebbero non essere protette e rendere pc, smartphone e tablet esposti a intrusioni esterne da parte di malintenzionati a caccia di dati personali. Inoltre, connessioni "infettate" da virus e malware potrebbero invitare gli utenti a installare un software prima dell'utilizzo, esponendo i dispositivi collegati a rischio di phishing.

8. Le foto delle vacanze e i tag. Non tutti vogliono apparire sui social network, essere riconosciuti o far sapere dove e con chi si trovavano durante le feste natalizie. Se si postano delle foto con altre persone, è meglio prima accertarsi che siano d'accordo, specie se si inseriscono anche dei tag con nomi e cognomi.

9. Geolocalizzazione solo quando si vuole. Se invece si preferisce non far sapere dove si è durante le vacanze o le feste di Natale si possono disattivare le opzioni di geolocalizzazione di smartphone e tablet e quelle dei social network utilizzati.

10. Smartphone e tablet protetti. Aggiornamenti software costanti e programmi antivirus dotati anche di anti-spyware e anti-spam possono essere delle buone precauzioni per evitare furti di dati o violazioni della privacy. Ma è bene ricordare che le migliori difese sono la consapevolezza nell'uso delle tecnologie e l'accortezza nel diffondere i nostri dati personali.

Per maggiori informazioni, è possibile consultare anche la sezione Diritti e Prevenzione del sito web www.garanteprivacy.it e le campagne di comunicazione del Garante **"Fatti smart"**, **"Connetti la testa" e "Spam: come difendersi"**.

E' inoltre possibile rivolgersi per informazioni, chiarimenti o segnalazioni all'**Ufficio Relazioni con il Pubblico (URP)** del Garante

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A cura del

Servizio relazioni con i mezzi di informazione

Copertina e impaginazione

Emiliano Germani

Stampa
IAG Mengarelli - Roma

Gennaio 2014

Per informazioni preso l'Autorità:
Ufficio per le relazioni con il pubblico Piazza di
Monte Citorio, 121
00186 Roma
Telefono: 06.696771 - 06.696772917
E-mail: urp@garanteprivacy.it
Posta elettronica certificata: urp@pec.gpdp.it

www.garanteprivacy.it
www.youtube.com/videogaranteprivacy
www.linkedin.com/company/autorit-garante-per-la-protezione-dei-dati-personali