le guide tematiche

#E-CONSUMER

La conoscenza, il primo acquisto da fare online

tutela della
PRIVACY
online

Testi
Codacons

Impaginazione
Nexidia Srl

LA PRIVACY AI TEMPI DI INTERNET
CONSIGLI UTILI PER IL CONSUMATORE DIGITALE

La sicurezza informatica è una questione sempre più sentita con il diffondersi dei servizi su internet, dall'home banking alle transazioni telematiche, dai blog ai social network.

Con la molteplicità di operazioni che ormai si svolgono su internet, un'enorme massa di dati, tra cui anche sensibili, transita in pochi secondi on line.

Si pensi che lo scambio di informazioni, reso intenso e pervasivo dalla Rete e dalle nuove tecnologie, comporta spesso la condivisione pubblica, in modo più o meno volontario, anche di materiale privato, come foto e messaggi personali.

Nell'attuale contesto multimediale, l'interessato ha, tuttavia, diritto di seguire la circolazione dei propri dati, venendo informato delle ragioni della loro acquisizione, delle modalità di trattamento, custodia, diffusione e comunicazione.

Ecco che allora, sempre maggiore attenzione deve essere dedicata, tra i tanti aspetti, anche dal singolo utente, alla tutela della propria privacy: diventa essenziale non tanto evitare che altri violino il pur diritto fondamentale di essere lasciati soli, quanto consentire che ogni individuo possa disporre di un agile diritto di controllo rispetto alle tante informazioni di carattere personale che altri possano aver assunto.

PRIVACY

La privacy si può definire come il diritto del soggetto a vedere tutelata la propria sfera privata. Il concetto è onnicomprensivo di molteplici aspetti: il diritto alla dignità umana, l'interesse alla riservatezza dei propri dati personali, la libertà da indebite influenze, il diritto a organizzare e controllare il proprio spazio di vita, sia esso fisico che digitale.

La tutela della privacy è garantita in capo all'utente che utilizza applicazioni internet con la finalità di assicurare che le informazioni che riguardano gli utenti vengano trattate nel rispetto delle norme che le regolano e, in particolare, nel rispetto dell'autodeterminazione del singolo alla loro diffusione e, contestualmente, nel controllo delle notizie che lo riguardano.

NORMATIVA E CODICE DELLA PRIVACY

L'Italia ha recepito nel proprio ordinamento le numerose direttive europee sulla materia: la normativa vigente va desunta dal d.lgs. n. 196 del 2003 (Testo Unico, entrato in vigore il 1° gennaio 2004), c.d. «Codice in materia di protezione dei dati personali». Il d.lgs. 196/2003 riconosce all'art. 1 il diritto del singolo sui propri dati personali affermando che *"Chiunque ha diritto alla protezione dei dati personali che lo riguardano".*

Il diritto sui propri dati è differente dal diritto alla riservatezza, in quanto non riguarda solamente informazioni inerenti la propria vita privata, ma si estende in generale a qualunque informazione relativa ad una persona, anche se non coperta da riserbo (sono dati personali ad esempio il nome o l'indirizzo della propria abitazione). A tal proposito, si distinguono:

- **dati personali:** qualunque informazione relativa a persona fisica,

ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (ex art. 4, lett. b), d. lgs. n. 196 del 2003)

• **dati sensibili:** i dati personali idonei a rivelare l'origine razziale, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (ex art. 4, lett. d), d. lgs. n. 196 del 2003);

• **dati identificativi:** i dati personali che permettono l'identificazione diretta dell'interessato (ex art. 4, lett. c), d. lgs. n. 196 del 2003);

• **dati anonimi:** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (ex art. 4, lett. n), d. lgs. n. 196 del 2003);

• **dati parasensibili:** si collocano a metà strada tra i dati anonimi ed i dati sensibili ed hanno la caratteristica di recare, comunque, pregiudizio ai diritti ed alle libertà dell'interessato.

Il Codice disciplina, inoltre, le diverse operazioni di gestione ("trattamento") dei dati, riguardanti la raccolta, l'elaborazione, il raffronto, la cancellazione, la modificazione, la comunicazione o la diffusione degli stessi.

Lo scopo della legge non è, dunque, quello di impedire il trattamento dei dati, ma di evitare che questo avvenga contro la volontà dell'avente diritto, ovvero secondo modalità pregiudizievoli.

Il Testo Unico definisce, pertanto:

• **diritti degli interessati**
• **modalità di raccolta e requisiti dei dati**
• **obblighi di chi raccoglie, detiene o tratta dati personali**
• **responsabilità e sanzioni in caso di danni**

ATTENZIONE: *Occorre pensare che spesso i siti sui quali l'utente naviga, i social network... hanno sede all'estero, così come i rispettivi server e, di conseguenza, in caso di violazioni della privacy non sempre si è tutelati da leggi italiane e europee.*

I siti che hanno sede in Italia e Europa sono invece sempre tenuti al rispetto delle normative nazionali e comunitarie vigenti ed è sempre presente un'Autorità di protezione dei dati (DATA PROTECTION AUTHORITY – In Italia: **Autorità Garante per la protezione dei Dati Personali**) a cui l'utente può rivolgersi e che potrà intervenire in caso di violazioni.

CHE COSA GARANTISCE LA NORMATIVA NAZIONALE E COMUNITARIA

A) LA SICUREZZA DEI DATI

La garanzia della sicurezza dell'informazione coincide con l'assicurare i requisiti di:

• **Riservatezza:** l'informazione deve essere accessibile solo a chi è autorizzato a conoscerla. Le informazioni riservate devono essere protette sia durante la trasmissione che durante la memorizzazione. I dati memorizzati devono essere protetti mediante crittografia (firma digitale) o utilizzando un controllo d'accesso, mentre per le informazioni riservate trasmesse è necessaria la crittografia.

• **Integrità:** le informazioni devono essere trattate in modo che siano difese da manomissioni e modifiche non autorizzate.
Per garantire l'integrità dei dati è necessario che il sistema sia preparato ad individuare eventuali modifiche apportate ai dati durante la trasmissione, sia intenzionalmente in seguito ad un attacco, sia involontariamente in seguito ad un errore di trasmissione.

• **Disponibilità:** l'informazione deve essere sempre disponibile alle persone autorizzate quando necessario.

B) L'INFORMATIVA

L'informativa deve essere idonea a rendere edotto l'interessato dell'identità del titolare del trattamento e dei diritti attribuiti dal codice stesso, nonché delle modalità per fruirne.

Gli elementi dell'informativa sono elencati nell'art. 13 del Codice della Privacy che, al comma I, così stabilisce: l'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

- **le finalità e le modalità** del trattamento cui sono destinati i dati
- **la natura obbligatoria o facoltativa** del conferimento dei dati
- **le conseguenze** di un eventuale rifiuto di rispondere
- **i soggetti o le categorie di soggetti** ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi
- **diritti di cui all'art. 7 Codice Privacy** (diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma

intelligibile, diritto di ottenere l'indicazione dell'origine dei dati personali; delle finalità e modalità del trattamento; della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati; diritto di ottenere: **a)** l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; **b)** la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati e l'attestazione di dette operazioni).

• **gli estremi identificativi del titolare** e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile

C) IL CONSENSO

Sulla base di una corretta informativa si può acquisire il consenso dell'interessato.

Per trattare dati diversi da quelli sensibili occorre un consenso espresso e almeno documentato per iscritto; per i dati sensibili ci vuole un consenso scritto dell'interessato e in più ci vuole anche l'autorizzazione del Garante.

Il codice attribuisce all'interessato i diritti di accesso, il diritto all'esattezza dei dati e alla legittimità del trattamento. Il diritto di accesso può riguardare anche dati valutativi. In mancanza di adesione del titolare del trattamento, l'interessato potrà ottenere la tutela dei propri diritti in via coattiva, mediante ricorso al Garante o in alternativa ricorso al tribunale. L'impresa che tratta i dati personali dei clienti deve,

quindi, considerare il principio generale per cui per trattare i dati personale occorre ottenere il preventivo consenso dell'interessato. Anche nel caso in cui il cliente abbia prestato il proprio consenso al trattamento dei dati, la loro diffusione deve rispettare i principi della pertinenza e non eccedenza degli stessi in riferimento alle finalità del trattamento. La persistenza negli archivi dei dati illegittimamente trattati è idonea, anche solo in potenza, a causare gravissimi danni all'immagine del soggetto leso.

Chi utilizza i dati personali di un soggetto è tenuto a rilasciare una informativa per illustrare le finalità e le modalità del trattamento dei dati, mentre il soggetto che conferisce i dati può verificare la correttezza del trattamento ed, in alcuni casi, revocare il proprio consenso al trattamento.

Nell'applicazione di queste regole al mondo virtuale si incontrano non pochi problemi, in quanto la rete internet per le sue particolari caratteristiche pone serie difficoltà nell'attuazione di forme di controllo.

L'idea di fondo che ha ispirato anche la normativa europea in materia privacy è quella che nell'odierna società dell'informazione la tutela dei dati personali non debba essere considerata come un ostacolo alla circolazione delle informazioni, ma come una delle regole utili ad un miglior funzionamento del sistema disciplinando e rendendo trasparente il flusso delle informazioni a garanzia e tutela degli interessati.

IL NUOVO REGOLAMENTO EUROPEO RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

L'esigenza di emanare un Regolamento Europeo in materia di protezione dei dati personali nasce dalla continua evoluzione degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente alla diffusione del progresso tecnologico.
Le nuove regole aggiornano la legislazione europea vigente, che risale alla Direttiva 95/46/CE che non teneva conto della rapida evoluzione delle tecnologie, né della grande mole di dati ora riversata in rete, spesso volontariamente dagli utenti – mediante social network ma non solo - e neanche dei nuovi dispositivi mobili, che hanno in modo imprevedibile accelerato le necessità di sicurezza
Il testo del Regolamento europeo in materia di protezione dei dati personali, ribadisce alcuni concetti fondamentali, che sono alla base della stessa Direttiva 95/46/CE e del Codice in materia di protezione dei dati personali.
Tra gli obiettivi fondamentali del Regolamento vi sono quelli di garantire certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese; offrire alle persone fisiche in tutti gli Stati membri il medesimo livello di azionabilità dei diritti; definire obblighi e responsabilità dei responsabili del trattamento e degli incaricati del trattamento ed assicurare un monitoraggio costante del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri.

Quali novità introduce il nuovo regolamento sulla Privacy?
Le nuove norme prevedono importanti novità:

Dovere di documentazione e di informazione la figura dell'Accountability (responsabilità del Titolare): il Titolare del trattamento dei dati deve conservare la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità, indicando obbligatoriamente - per ognuno di essi - una serie "nutrita" di informazioni, tali da assicurare e comprovare la conformità di ciascuna operazione alle disposizioni del Regolamento.

Privacy by design e Privacy by default: si tratta di nuovi obblighi che il Titolare avrà ancor prima di procedere al trattamento dei dati. Dovrà cioè pensare in un'ottica di Privacy già dal momento in cui disegna il nuovo hardware o software o semplicemente il nuovo servizio. Inoltre, dovrà pensarlo con tutte le impostazioni di Privacy "chiuse" e non "aperte", come si è fatto finora (basti pensare a Facebook o ad altri social).

Data Protection Officer: è una nuova figura di super consulente che ogni Titolare, che sia una Pubblica Amministrazione o un ente (Società, associazione o Professionista) che tratti dati di oltre 5000 o 50.000 interessati, deve avere. Il soggetto incaricato deve assicurare la conformità a tutte le regole e il suo nome deve essere comunicato all'Autorità Garante per la Protezione dei Dati Personali.

Valutazione di impatto: si deve prevedere prima dell'inizio del trattamento una valutazione dei possibili rischi che questo comporta e occorre prevederne le misure correttive e le eventuali comunicazioni al Garante. La valutazione va documentata per iscritto.

Informative e consenso: le informative all'interessato dovranno essere più dettagliate, ma soprattutto più efficaci delle precedenti, usando anche moduli, schemi e disegni. Il consenso, invece, dovrà essere sempre espresso in modo inequivocabile e non dovrà essere una possibilità per effettuare trattamenti illeciti.

Obblighi di segnalazione in caso di Violazione sui dati: Con la nozione di violazione dei dati personali (c.d. "personal data breaches"), si intende: la distruzione, la perdita, la modifica, la rivelazione

non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati.
I Titolari del trattamento, in caso di una violazione come sopra descritta, dovranno mettere in atto due differenti azioni: la notificazione della violazione all'Autorità di controllo e la segnalazione al diretto interessato.

Diritto all'oblio: l'interessato ha il diritto di ottenere, dal responsabile del trattamento, la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati, in particolare in relazione ai dati personali resi pubblici quando l'interessato è un minore. Quando ha reso pubblici dati personali, il responsabile del trattamento prende tutte le misure ragionevoli, anche tecniche, in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto responsabile di tale pubblicazione.

Diritto alla portabilità del dato: l'interessato ha il diritto, ove i dati personali siano trattati con mezzi elettronici di uso comune, di ottenere dal responsabile del trattamento copia dei dati trattati in un formato elettronico e strutturato che sia di uso comune e gli consenta di farne ulteriore uso.

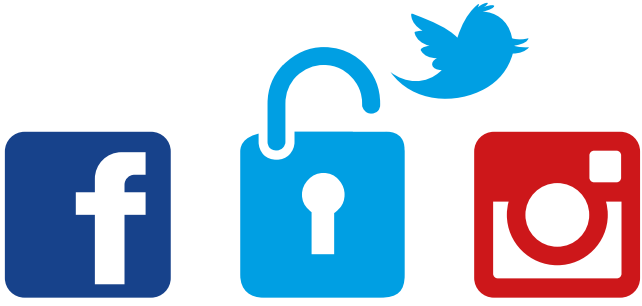
Le previsioni del citato regolamento interesseranno tutti quei soggetti (anche extraeuropei) che sono chiamati a trattare (in maniera automatizzata o meno) i dati relativi, per esempio, a clienti, dipendenti, studenti, utenti, fornitori. In sostanza, viene introdotto il principio dell'applicazione del diritto dell'Unione Europea anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o sevizi a cittadini UE o tali da comportare il monitoraggio dei loro comportamenti.

Il Regolamento si applica anche al trattamento di identificativi prodotti da dispositivi, applicazioni, strumenti e protocolli, quali gli indirizzi IP, i cookies e i tag di identificazione a radiofrequenza, salvo il caso in cui tali identificativi non si riferiscano a una persona fisica identificata o identificabile.

Le aziende e le istituzioni pubbliche dovranno, pertanto, adottare politiche ed attuare misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato sia conforme - fin dalla fase embrionale - a tutte le disposizioni del Regolamento.

LA PRIVACY NEI SOCIAL NETWORK

Particolarmente sentito è il problema della tutela della privacy nell'utilizzo dei social network: i rischi sono molto elevati; si pensi, ad esempio che nel momento in cui ci si iscrive a social network (Facebook, Twitter...), in automatico e senza che l'utente abbia previamente ed espressamente manifestato il proprio consenso quest'ultimo vedrà indicizzato il prorpio nome sui motori di ricerca



estranei al network , cosicché immagini e dati personali potranno essere visibili a chiunque – anche non iscritto al medesimo social – digiti il nome sul motore di ricerca.

Inoltre, neppure è semplice cancellare detti dati. Infatti, sulla pagina principale (es. Facebook) non sono riportate le informazioni sula possibilità di recedere: l'account può essere cancellato, solo all'interno delle pagine personali, accedendo all'area "impostazioni".

Ma non è finita.

Tutte le informazioni, le immagini e i dati personali non vengono rimossi al momento della disattivazione dell'account ma rimangono sul server.

Dati i rischi, è necessario che, da un lato, i fornitori dei servizi di social network assicurino la massima trasparenza delle informazioni agli utenti e rendano più semplici le operazioni di recesso dal servizio ma, dall'altro, è necessario un uso attento e consapevole dello strumento da parte dell'utente stesso.

In particolare, è necessario:

- **controllare effettivamente e periodicamente i dati** e le informazioni personali condivise e la loro diffusione: basta pensare che data e luogo di nascita sono sufficienti a risalire al codice fiscale
- **aumentare i livelli di privacy del 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

• **limitare al massimo la disponibilità di informazioni,** soprattutto per quanto riguarda la reperibilità dei dati da parte dei motori di ricerca
• **impostare misure di controllo** al fine di impedire gli accessi abusivi ai profili-utente da parte di soggetti terzi, ad esempio mediante dispositivi di spidering
• **astenersi dal pubblicare informazioni personali** e foto relative ad altri (magari "taggandone" i volti) senza il loro consenso

LA PRIVACY NELL'E COMMERCE

Altro settore in cui particolare attenzione deve essere dedicata alla tutela della privacy dell'utente – consumatore è quello dell'e commerce.

Con l'espressione inglese e-commerce (commercio elettronico) ci si riferisce, tipicamente, alla compravendita di beni e servizi commercializzati attraverso piattaforme online.

La vendita on line è quella vendita effettuata tramite Internet, mediante accesso del compratore al sito web del venditore e si riferisce a quell'insieme di pratiche dirette alla commercializzazione di un bene o di un servizio per via telematica (tramite Internet, invio di e-mail alla clientela, ecc.).

La prassi del commercio elettronico è, senza dubbio, caratterizzata da numerose occasioni di raccolta dei dati personali del naviga-

tore-consumatore «virtuale», ora palesi – mediante la richiesta di compilazione di generici formulari elettronici o di veri e propri ordini di beni o servizi – ora occulte – si pensi al caso emblematico della raccolta automatica di dati personali mediante i c.d. cookie.
Per un utilizzo consapevole di tale strumento, occorre:

- **utilizzare password imprevedibili e con codici alfanumerici,** cambiandole frequentemente e diversificandole a seconda dei siti
- **evitare di comunicare la propria password** e conservarla in un luogo sicuro, non sul computer che va in rete
- **installare e configurare firewall e antivirus**
- **procurarsi un antispyware** in grado di ripulire efficacemente il sistema
- **tenere sotto controllo i cookies**
- **utilizzare un trace eraser** per cancellare tracce elettroniche
- **non aprire allegati di e-mail** provenienti da utenti sconosciuti o sospetti
- **leggere le licenze** e le disposizioni riguardo alla privacy prima di installare un qualsiasi software
- **segnalare al Garante Privacy e alle autorità competent**i (es. Polizia Postale), eventuali violazioni.

LA PRIVACY NELL'HOME BANKING

Il problema della privacy riguarda la tutela dei propri dati finanziari.
Si parla di e-banking (electronic banking) per indicare i servizi bancari che sono forniti elettronicamente, per esempio tramite Internet.
Per permettere ai servizi di funzionare, è necessario però che si crei un rapporto di fiducia tra banca e cliente e per far si che ciò avvenga è necessario che sia garantito il rispetto di criteri di sicurezza per il corretto svolgimento delle operazioni (impiego della crittografia, elaborazione di protocolli di trasmissione sicuri).

È sempre però necessario che l'Utente adotti alcuni importanti accorgimenti:

1. **Diffidare da richieste di dati relativi a carte di pagamento,** chiavi di accesso all'home banking o altre informazioni personali perché la propria banca non richiederà mai tali informazioni;
2. **Connettersi al sito della banca**, scrivendo direttamente l'indirizzo nella barra di navigazione e non cliccare su link presenti in e-mail sospette, perché potrebbero condurre a siti contraffatto,.
3. **Controllare regolarmente le movimentazioni** del conto corrente;
4. **Diffidare da messaggi** provenienti da posta elettronica, siti web, contatti di instant messaging, che invitano a scaricare programmi o documenti di cui ignori la provenienza.
5. **Fare attenzione** se viene richiesto l'inserimento dei dati personali sul tuo sito di home banking in modo diverso dal consueto;
6. **Non divulgare i dati** (PIN, CODICI DI SICUREZZA) senza essere sicuro dell'identità di chi li sta chiedendo.

#E-CONSUMER
La conoscenza, il primo acquisto da fare online

Spesa finanziata dal Ministero
dello Sviluppo Economico
ai sensi del Decreto 6 agosto 2015

CODACONS

Viale Mazzini 73 - 00195 Roma
tel. 06.3728667 - fax 06.3701709
info@codacons.it • www.codacons.it
facebook.com/Codacons

MOVIMENTO DIFESA del Cittadino

Via Carlo Felice 103 - 00185 Roma
tel 06.4881891 - fax 06.42013163
info@mdc.it • www.difesadelcittadino.it
facebook.com/movimentodifesadelcittadino

Associazione Utenti dei Servizi Radio Televisivi

Via Andreoli 2 - 00195 Roma
tel 06.62289628
info@utentiradiotv.it • www.utentiradiotv.it
facebook.com/utentiradiotv