PRIVACY E NUOVE TECNOLOGIE: COSA DEVI SAPERE

unolegal
Privacy Solutions

App & Privacy:
Aspetti regolamentari e best practice

Sommario

1. Che cosa sono le APP
2. Come funziona una APP ed esempi di dati trattati
3. Parti coinvolte nel trattamento dei dati
4. Consigli sull'uso delle APP e considerazioni finali

1. Che cosa sono le APP

Le **APP** sono applicazioni software per dispositivi mobili che organizzano informazioni e dati e forniscono all'utente determinati servizi e funzioni. Tali applicazioni sono in grado di raccogliere **grandi quantità di dati dal dispositivo** (ad esempio dati memorizzati dall'utente e dati da diversi sensori, tra cui la geolocalizzazione) e di elaborarli per fornire servizi nuovi e innovativi all'utente finale.

Dato il loro **crescente aumento** e le ragioni del successo legate al **basso costo** (o a titolo gratuito) e la **facilità di utilizzo**, è importante chiarire il **quadro giuridico** applicabile al trattamento dei dati personali nelle fasi di sviluppo, distribuzione e utilizzo di applicazioni su dispositivi intelligenti. E' necessario concentrarsi in particolare sul requisito del consenso, sui principi di limitazione della finalità e di minimizzazione dei dati, sulla necessità di prendere misure di sicurezza adeguate, sull'obbligo di informazione corretta agli utenti finali, sui relativi diritti, sui periodi ragionevoli di conservazione dei dati e, nello specifico, sull'equo trattamento dei dati provenienti da minori e relativi ad essi.

Il quadro normativo di riferimento è ampio, composto dalla Direttiva UE così detta e-Privacy, da Pareri e Raccomandazioni del Gruppo Art. 29, dal Codice Privacy e da alcuni Provvedimenti Specifici dell'Autorità Garante e da alcune Best Practice da tenere in considerazione.

- *La tua azienda è consapevole dei propri obblighi Privacy derivanti dall'uso di una App?*

- *La tua azienda è consapevole che l'uso di una App consente di avere accesso e processare una mole sterminata di dati (anche personali) presenti all'interno di un dispositivo?*

2. Come funziona una APP ed esempi di dati trattati

Le App sono applicazioni software destinate a una serie particolare di dispositivi intelligenti, quali **smartphone, tablet** e organizzano le informazioni in modo adatto alle caratteristiche specifiche del dispositivo, interagendo spesso strettamente con l'hardware e il sistema operativo presente sul dispositivo.

Il sistema operativo (**S.O.**) dei dispositivi mobili è poi progettato per mettere a disposizione delle App attraverso interfacce di programmazione dell'applicazione (**API**), una moltitudine di componenti (rubrica, giroscopio, bussola digitale, messaggi, fotocamera, microfono, WI-Fi, Bluetooth, servizi di geolocalizzazione, etc.).

Siamo quindi in presenza di una stretta interazione tra App e S.O. del dispositivo mobile, per mezzo della quale gli sviluppatori di applicazioni sono in grado di raccogliere continuamente dati (anche personali), presenti nel dispositivo.

Esempi di dati personali che possono influire in misura significativa sulla vita privata degli utenti finali e altri individui sono i seguenti:

1. Ubicazione;
2. Contatti;
3. Identità dell'interessato;
4. Carta di credito e dati di pagamento;
5. Cronologia di navigazione;
6. Credenziali di autenticazione per i servizi web e social;
7. Fotografie e filmati.

3. Parti coinvolte nel trattamento dei dati

I soggetti coinvolti nello sviluppo, nella distribuzione e nella gestione di applicazioni sono numerosi e con responsabilità differenti in fatto di protezione dei dati.
Si possono comunque ricondurre alle seguenti figure:

a) App Developers

Sono coloro i quali sviluppano le applicazioni, creano App e/o le mettono a disposizione di utenti finali. Progettando e/o creando il software che girerà sugli smartphone, decidono in che misura l'applicazione potrà accedere a diverse categorie di dati personali e procedere al loro trattamento, nel dispositivo e/o attraverso risorse informatiche remote. Nella misura in cui determinano le **finalità** e i **mezzi del trattamento di dati personali** su dispositivi intelligenti, lo sviluppatore di applicazioni deve essere considerato il **Titolare del trattamento.**

b) Produttori di S.O. e dispositivi mobili

Anche i produttori di S.O. e dispositivi devono essere considerati **Titolari del trattamento** di eventuali dati personali trattati per **finalità proprie**, quali il regolare funzionamento del dispositivo, la sicurezza o i dati personali trattati in seguito all'installazione o all'utilizzo di applicazioni.

c) App store

I dispositivi intelligenti più diffusi hanno tutti un proprio **App store** e capita di frequente che un particolare sistema operativo sia profondamente integrato con un particolare App store. Spesso gli App store gestiscono i pagamenti per le applicazioni e possono anche supportare acquisti che richiedono la registrazione dell'utente con nome, indirizzo e dati finanziari. Per quanto concerne il trattamento e le finalità proprie connesse a questi dati personali, gli App store si possono considerare **Titolari** del trattamento dei dati.

d) Terzi parti

I terzi coinvolti nel trattamento dei dati attraverso l'utilizzo di applicazioni sono numerosi. Ad esempio, possono essere identificati come *Intermediari di pubblicità* (Banner dentro App) o come *Fornitori di servizi analitici* (per info sull'uso, sulla popolarità e fruibilità delle App).

- *In quale di queste quattro figure si identifica la tua azienda?*

4. Consigli sull'uso delle APP e considerazioni finali

Tre i **principi** fondamentali da rispettare: **l'Informativa** in merito al trattamento dei dati che dovrà essere fornita all'utente prima della stessa installazione dell'APP; il relativo **Consenso** per il quale il semplice "click" sul pulsante "Installa" non si può considerare una valida autorizzazione al trattamento dei dati; il **Diritto di Accesso** ai propri dati che dovrà essere comunque garantito anche attraverso lo stesso "App store" dal quale l'APP è stata scaricata.

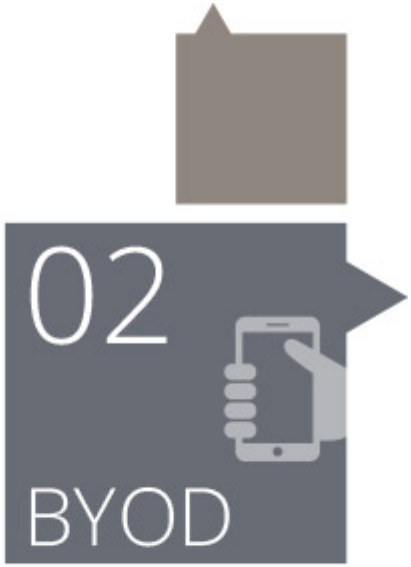
- *E se l'APP dovesse trattare i dati personali raccolti anche per finalità volte all'analisi dei consumi e delle abitudini degli utenti per ricostruirne un profilo di consumo e non solo?*

- *La tua azienda è consapevole delle implicazioni Privacy derivanti dall'uso delle App che permettono un trattamento di dati personali (es. dei dipendenti) attraverso la geolocalizzazione?*

Proprio con riferimento a quest'ultimo punto, gli **accertamenti** compiuti dall'Autorità Garante hanno riguardato l'uso dei sistemi di localizzazione satellitare (GPS) nell'ambito del rapporto di lavoro.

I principali motivi per le quali le aziende sono state sanzionate hanno riguardato il mancato adempimento dell'obbligo di **notificazione** ai sensi dell'art. 37 del Codice Privacy, la mancata nomina a **responsabile** del trattamento verso il fornitore della tecnologia.

- *La tua azienda è a conoscenza dei rischi e delle implicazioni Privacy:*
  - sull'errato sviluppo ed utilizzo di una APP?
  - sulla mancanza di trasparenza e di informazioni per gli utenti?
  - sull'incertezza delle finalità del trattamento?
  - in assenza di un consenso libero e informato prima del trattamento?
  - in presenza di scarse misure di sicurezza?
  - in caso di processi di massimizzazione dei dati?



Come implementare nella pratica il BYOD (Bring Your Own Device) in azienda?

Sommario

1. Che cos'è il "BYOD"?

Un dato è ormai certo: l'utilizzo del "**BYOD**" **(Bring Your Own Device)** tra le aziende risulta essere ancor di più oggi un successo a livello globale. La tendenza ad utilizzare il computer o dispositivo mobile personale sul posto di lavoro, è diventata talmente diffusa che da opzione volontaria, autorizzata dalle aziende, si sta trasformando in una scelta obbligata, indirizzata dai datori di lavoro.

Il **lavoratore**, in tale contesto, può connettersi a risorse informative e documentali aziendali, mediante l'utilizzo del **proprio dispositivo mobile**, per lo svolgimento dell'attività lavorativa. In altri termini, il lavoratore accede alle reti e ai contenuti di **proprietà dell'azienda,** conserva e tratta informazioni e applicazioni aziendali attraverso l'utilizzo del **proprio apparecchio**.

L'utilizzo di tale servizio, fino a qualche anno fa, sembrava (quasi) di avanguardia fantascientifica. Oggi, questa tecnologia offre soluzioni formidabili, efficienti ed efficaci, ma rappresenta anche la nuova frontiera del rischio regolatorio e legale, amministrativo e penale prima di tutto, per qualsiasi azienda e singolo consulente o responsabile di progetti.

Anche nei documenti ufficiali del **Garante per la Protezione dei Dati Personali** si parla di BYOD: sia nel Provvedimento generale in tema di **biometria** del 12/11/2014 sia nelle Linee-guida in materia di **riconoscimento biometrico e firma grafometrica**. In entrambi gli ambiti l'Autorità considera il significativo sviluppo nel settore IT rispetto all'utilizzo, per finalità aziendali, di dispositivi mobili di proprietà del dipendente o del collaboratore.

La tua azienda consente ai propri dipendenti e collaboratori di utilizzare i propri dispositivi mobili personali (tablet, smartphone e laptop) per scopi di lavoro?

2. Le definizioni importanti

Quando si parla di BYOD occorre avere chiaro il significato e il perimetro dei suoi 3 elementi costitutivi e cioè:

1. **Cosa si intende per dispositivi mobili**? Una corretta interpretazione della definizione di BYOD impone di restringere il campo d'applicazione a telefoni cellulari, smartphone, PDA e tablet, dispositivi "portatili" dotati di sistema operativo proprio, diverse funzionalità informatiche (ad es. Wi-Fi, GPS, fotocamera) ed in grado di supportare applicazioni software (App);
2. **È applicabile solo ai dipendenti**? Le Politiche di BYOD, interessano ogni "lavoratore" che opera per conto di un soggetto, indipendentemente dall'esistenza di un contratto di lavoro subordinato (ad es. contratti a progetto) o autonomo (ad es. consulenti, professionisti);
3. **Quali informazioni aziendali devo tutelare**? Le informazioni/dati relativi e/o comunque connessi in modo funzionale all'organizzazione aziendale.

3. Perché e come utilizzarlo

Il BYOD determina un aumento sia della **produttività**, in considerazione del fatto che il dipendente utilizza un dispositivo mobile di sua proprietà (evitando il doppio uso, del personale e dell'aziendale) che **dell'innovazione** aziendale grazie ai continui aggiornamenti software a cui vengono sottoposti, con conseguenti vantaggi anche per l'azienda.

Da non sottovalutare poi l'aspetto della **riduzione dei costi** in considerazione che sarà l'utente/lavoratore a sostenere le spese di acquisto, gestione e aggiornamento del dispositivo mobile.

Da ultimo, si può approfittare dell'occasione del suo utilizzo per elevare gli **standard di**

sicurezza aziendali dal punto di vista della protezione dei dati personali, stabilendo, ad esempio, quali tipologie di dati personali possono essere conservati sui dispositivi mobili di proprietà del lavoratore e quali invece no (ad es. i dati sensibili).

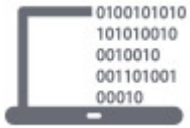
La tua azienda è consapevole dei vantaggi derivanti dal punto di vista della protezione dei dati personali?

Non meno rilevante è però l'aspetto, critico, derivante **dall'uso promiscuo** e per finalità differenti (lavorative e personali) dei dispositivi mobili da parte dei lavoratori.

È bene sottolineare che, benché sia il dipendente/lavoratore a gestire e utilizzare per fini aziendali il dispositivo di sua proprietà, è il **datore di lavoro/impresa** il soggetto obbligato alle prescrizioni e regole previste dal **Codice della Privacy** e a ogni altro obbligo previsto dalla normativa in materia di protezione dei dati personali.

La tua azienda è altrettanto consapevole dei rischi?

4. Suggerimenti pratici



Un'efficace politica BYOD non dovrebbe prescindere all'azienda dall'affrontare e dal rispondere alle seguenti domande:

1. È ben chiara la suddivisione tra **dispositivi di proprietà aziendale** e **dispositivi personali**?
2. Sono state specificate le tipologie di dati personali/informazioni che non è consentito **conservare all'interno del dispositivo personale**? Un'efficace politica di BYOD, ad esempio, può stabilire il divieto di salvare dati sensibili o informazioni riservate dell'azienda all'interno del dispositivo personale, a meno che non siano state salvate all'interno di una infrastruttura IT di proprietà dell'azienda;
3. È stata predisposta una **Policy delle politiche di BYOD** coerente ed integrata con le Policy aziendali già esistenti?
4. All'interno della Policy ovvero dei contratti di lavoro è specificato **l'obbligo in capo al lavoratore di informare l'azienda** di ogni effettivo o sospetto avvenimento di hacking e/o di rivelazione non autorizzata di dati contenuti all'interno del dispositivo mobile?
5. Sono affrontati gli aspetti relativi alla **sicurezza dei dispositivi mobili**, implementando, ad esempio, protezione con password, cifratura dei dati, connessioni sicure?
6. Si utilizzano **servizi Cloud**? In quali Paesi avviene il **trasferimento dei dati**? Sono Paesi che offrono o meno un "adeguato" livello di protezione dei dati?
7. Si tengono in considerazione anche le implicazioni e i limiti imposti dalle **normative a tutela dei lavoratori in tema di "controlli"**?

5. Considerazioni finali

Il BYOD è sinonimo di produttività. Ma anche una **sfida ancora da vincere.** È uno scenario a luci e ombre, che premia le "virtù" del BYOD da una parte e ne condanna i "limiti" dall'altra. Un po' come successe al Cloud Computing qualche anno fa. Il BYOD è l'opportunità che le Aziende hanno di integrare la "**Privacy**" all'interno delle proprie attività, facendone cosi un fattore distintivo (**Privacy as an Asset**) in grado di differenziarla sul mercato dai propri competitors.

Privacy e Cloud Computing

Sommario

1. Il Cloud Computing
2. I principali rischi
3. I contratti Cloud

1. Il Cloud Computing

Un insieme di tecnologie e modalità di fruizione di servizi informatici che favoriscono l'utilizzo di software, la conservazione e l'elaborazione di grandi quantità di informazioni via Internet.

"*I servizi offerti dai fornitori di soluzioni di Cloud Computing sono molto diversificati e spaziano da sistemi elaborativi virtuali (che sostituiscono o si affiancano ai tradizionali server controllati direttamente dal responsabile del trattamento dei dati) a servizi di supporto allo sviluppo e per l'hosting evoluto delle applicazioni, sino a soluzioni software rese disponibili in modalità web che sono sostitutive delle tradizionali applicazioni installate sui computer degli utenti finali, quali ad esempio applicazioni per l'elaborazione dei testi, per la gestione di agende e calendari, cartelle per l'archiviazione dei documenti on-line e soluzioni esternalizzate di posta elettronica*" (Fonte: Gruppo di Lavoro Articolo 29 per la Protezione dei Dati).

A partire dal 1° luglio 2012, il **rischio legale** del ricorso a tale tecnologia è misurabile grazie al Parere 05/2012 del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, all'interno del quale sono presenti le raccomandazioni per un uso "consapevole" di tale tecnologia. Nell'ambito del Cloud Computing è possibile distinguere tra:

- **Private Cloud**: un'infrastruttura rivolta ad una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo (hosting) nei confronti del quale il titolare dei dati può esercitare un controllo puntuale. Può essere paragonata ai tradizionali "data center" nei quali sono usati degli accorgimenti tecnologici che ottimizzano l'utilizzo delle risorse e le potenziano attraverso investimenti contenuti e progressivi nel tempo.
- **Public Cloud**: un'infrastruttura di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni i propri sistemi attraverso l'erogazione via web l'utilizzo delle risorse disponibili.

2. I principali rischi

Imprese e amministrazioni che intendono utilizzare servizi di Cloud Computing dovrebbero innanzitutto effettuare un'**analisi del rischio** completa e approfondita.

Malgrado i vantaggi riconosciuti del Cloud Computing in termini economici e sociali, la diffusione su vasta scala dei servizi di Cloud Computing comporta una serie di rischi per la protezione dei dati.

Di seguito alcuni tra i principali:

1. La mancanza di **controllo esclusivo** dei dati da parte del Cliente/Titolare del trattamento;
2. Quale **diritto** è applicabile nei casi di Titolari del trattamento con una o più sedi anche **all'interno della UE**;
3. Quali sono i **ruoli** e le **responsabilità** del cliente Cloud e del fornitore Cloud;

Il contratto Cloud stipulato dalla tua azienda permette una chiara identificazione e allocazione delle responsabilità dei soggetti coinvolti?

4. Come gestire il servizio di Cloud Computing che comporta il coinvolgimento di **subfornitori**;
5. Il diritto dell'interessato alla cancellazione dei propri dati personali;
6. Come gestire il trasferimento dei dati verso **paesi extra-UE**

3. I contratti Cloud

Quando ci si affida a servizi di Cloud Computing, i titolari del trattamento devono **scegliere un fornitore** che presenti garanzie sufficienti in merito alle misure di **sicurezza tecnica** e all'organizzazione dei trattamenti da effettuare e devono assicurarsi del rispetto di tali misure. Inoltre, sono obbligati a firmare un contratto formale con il fornitore di servizi Cloud,

che stabilisca che la relazione tra Titolare/Cliente e Responsabile/Fornitore sia disciplinata da un **contratto** o un altro atto giuridico vincolante. Al fine di garantire la certezza giuridica, il contratto deve prevedere, tra gli altri, anche i seguenti aspetti:

- Gli accordi sul livello del servizio (SLA) applicabili (che dovrebbero essere oggettivi e misurabili) e le sanzioni pertinenti;
- Oggetto e orizzonte temporale del servizio Cloud da fornire;
- Obbligo del fornitore Cloud di fornire un elenco dei luoghi dove può avvenire il trattamento dei dati.

- *La tua azienda è consapevole ed è a conoscenza degli altri aspetti da considerare?*

- *La tua azienda ha predisposto una checklist Privacy (es. misure di sicurezza predisposte) contenente gli elementi che occorre valutare e analizzare attentamente?*

Infine, la **verifica** o la **certificazione** indipendente effettuata da un terzo affidabile può essere uno strumento credibile per i fornitori Cloud per dimostrare la conformità con gli obblighi posti a loro carico. Tale ipotesi potrebbe servire a indicare che i controlli in materia di protezione dei dati sono stati oggetto di **audit** a fronte di una norma riconosciuta e conforme ai requisiti indicati nel Parere 05/2012 del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati.

Cookie e applicazioni web: l'intervento del legislatore

Sommario

1. Che cosa sono i cookie
2. Le tipologie di cookie
3. L'informativa di primo e secondo livello e il consenso
4. La Notificazione
5. Suggerimenti pratici e considerazioni finali

1. Che cosa sono i cookie

In data 3 giugno 2014 è stato pubblicato nella G.U il **Provvedimento del Garante 8 maggio 2014, n. 214 "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie**. Con tale Provvedimento vengono inoltre stabilite le regole per una gestione semplificata dell'informativa e del consenso.

Che cosa sono i **cookie**? I **cookie** sono stringhe di testo di piccole dimensioni che i siti visitati dall'utente inviano al suo terminale (solitamente al browser), dove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente.

Nel corso della navigazione su un sito, l'utente può ricevere sul suo terminale anche cookie che vengono inviati da siti o da web server diversi (c.d. "**terze parti**"), sui quali possono risiedere alcuni elementi (quali, ad esempio, immagini, mappe, suoni, specifici link a pagine di altri domini) presenti sul sito che lo stesso sta visitando.

I cookie, solitamente presenti nei browser degli utenti in numero molto elevato e a volte anche con caratteristiche di ampia persistenza temporale, sono usati per **differenti finalità**: esecuzione di autenticazioni informatiche, monitoraggio di sessioni, memorizzazione di informazioni su specifiche configurazioni riguardanti gli utenti che accedono al server, ecc.

Il tuo sito web è già allineato alla nuova normativa?

2. Tipologie di cookie

Al fine di giungere a una corretta regolamentazione, è necessario distinguere i cookie sulla base delle finalità perseguite da chi li utilizza, **posto che non vi sono delle caratteristiche tecniche che li differenziano gli uni dagli altri.**

Al riguardo, si individuano pertanto **due macro-categorie**:
a) cookie "**tecnici**"
b) cookie di "**profilazione**"

In **assenza dei primi** alcune operazioni risulterebbero complesse o impossibili da eseguire (es. autenticazioni informatiche). **I secondi** sono spesso utilizzati dai siti per raccogliere importanti informazioni all'insaputa degli utenti sui loro gusti, sulle loro abitudini, sulle loro scelte.

I **cookie tecnici** sono normalmente installati direttamente dal titolare o gestore del sito web e possono essere suddivisi in: **cookie di navigazione o di sessione**, **cookie analytics**, **cookie di funzionalità**. Per l'installazione di tali cookie **non è** richiesto il preventivo **consenso** degli utenti e resta fermo **l'obbligo di dare l'informativa** ai sensi dell'art. 13 del Codice, che il gestore del sito, qualora utilizzi soltanto tali dispositivi, potrà fornire con le modalità che ritiene più idonee.

I **cookie di profilazione** sono volti a creare profili relativi all'utente e vengono utilizzati al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dallo stesso nell'ambito della navigazione in rete. In ragione della particolare invasività che tali dispositivi possono avere nell'ambito della sfera privata degli utenti, la normativa europea e italiana prevede che l'utente debba essere adeguatamente informato sull'uso degli stessi ed esprimere così il proprio valido consenso.

Per l'installazione di tali cookie **è richiesto** il preventivo **consenso** degli utenti, e resta fermo **l'obbligo di dare l'informativa** ai sensi dell'art. 13 del Codice, che il gestore del sito, qualora utilizzi soltanto tali dispositivi, potrà fornire con le modalità che ritiene più idonee.

- *Il tuo sito web prevede l'utilizzo di cookie di profilazione?*
- *Hai già individuato le modalità semplificative per l'informativa e l'acquisizione del consenso?*

3. L’informativa di primo e secondo livello e il consenso

Ai fini della semplificazione dell'**informativa**, il Garante ritiene che una soluzione efficace, che fa salvi i requisiti previsti dall'art. 13 del Codice (compresa la descrizione dei singoli cookie), sia quella di impostare la stessa su **due livelli** di approfondimento successivi.

Nel momento in cui l'utente accede a un sito web, deve essergli presentata una prima informativa "**breve**", di *primo livello*, contenuta in un **banner** a comparsa immediata sulla home page (o altra pagina tramite la quale l'utente può accedere al sito), contenente l’indicazione, tra le altre: che il sito utilizza **cookie di profilazione** al fine di inviare messaggi pubblicitari in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete oppure che il sito consente anche l'invio di cookie "**terze parti**" (laddove ciò ovviamente accada);

- *Il tuo sito web, alla home page, prevede un banner contenente la prima informativa "breve” per i cookie?*

- *Il tuo sito web prevede la possibilità di negare il consenso a tutti i cookie?*

L’informativa breve deve essere poi integrata da un'informativa "**estesa**", alla quale si accede attraverso un **link** cliccabile dall'utente e raggiungibile da ogni pagina del sito (ad esempio, inserendo il link nel footer di ogni pagina del sito) e che, tra gli altri: contenga tutti gli elementi previsti dall'**art. 13** del Codice; contenga al suo interno anche il link aggiornato alle informative e ai moduli di consenso delle terze parti con le quali il gestore del sito ha stipulato accordi per l'installazione di cookie tramite il proprio sito.

- *Hai già pensato all’utilizzo di un cookie tecnico per tenere traccia del consenso dell’utente?*

4. La Notificazione

Il Provvedimento ricorda che l'uso dei cookie rientra tra i trattamenti soggetti all'obbligo di **Notificazione al Garante** ai sensi dell'art. 37, comma 1, lettera d), del Codice, laddove lo stesso sia finalizzato a "*definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti*".

Dal quadro sopra delineato, emerge pertanto che, mentre i **cookie di profilazione** sono soggetti all'obbligo di notificazione, i cookie che invece hanno finalità diverse e che rientrano nella categoria dei **cookie tecnici**, ai quali sono assimilabili anche i **cookie analytics**, non debbano essere notificati al Garante.

Lo sai che, in caso di utilizzo di cookie di profilazione di terze parti, la Notificazione al Garante è a carico del soggetto terza parte che svolge l'attività di profilazione?

5. Suggerimenti pratici e considerazioni finali

Un'efficace analisi aziendale sui cookie non dovrebbe prescindere:

- Da una **capillare** verifica interna su quali cookie vengono serviti;
- Dalla considerazione che il rischio che vengano emesse **sanzioni** da parte delle autorità Garanti locali è in aumento;
- Dalla considerazione che le **imprese multinazionali** devono implementare una strategia coordinata di gestione dei cookie.

La disciplina specifica per i cookie ha introdotto il cosiddetto **principio dell'opt-in** rispetto ai cookie non strettamente necessari (per esempio, per cookie pubblicitari) il cui impiego deve

essere debitamente consentito dall'utente attraverso un consenso esplicito.
Ove l'utente negasse il proprio consenso, ciò non dovrebbe comunque impedirgli di navigare su quel sito internet.
Derogano al principio del previo consenso quei cookie che siano necessari per il funzionamento del sito internet e quelli necessari a fornire il servizio esplicitamente richiesto dall'utente.

Il momento in cui verranno implementate tali misure costituirà una sorta di "anno zero" per la gestione e relativa memorizzazione dei cookie dei visitatori del sito.
Il **termine ultimo** di adeguamento era fissato per il **3 giugno 2015**.

Privacy e Social Media

Sommario

1. I Social Media come strumento di comunicazione

"Il social network on-line può essere definito sostanzialmente come una piattaforma di comunicazione on-line che consente ad un utente di creare reti di utenti che condividono i suoi stessi interessi o di entrarne a far parte".

"Gran parte degli introiti dei Social network on-line è assicurata dalla pubblicità proposta sulle pagine web che gli utenti pubblicano e consultano. Gli utenti che inseriscono nel proprio profilo grandi quantità di dati sui loro interessi rappresentano un ricco mercato per gli inserzionisti, che sulla base di tali dati possono proporre pubblicità mirata". "È quindi importante che gli SNS operino nel rispetto dei diritti e delle libertà degli utenti, i quali si aspettano legittimamente che i loro dati personali siano elaborati conformemente alla legislazione europea e nazionale sulla protezione dei dati e sulla Privacy" (Fonte: Gruppo di Lavoro Articolo 29 per la Protezione dei Dati).

Il social network rappresenta oggi uno strumento di comunicazione dalla enorme efficacia e dalle enormi potenzialità, in considerazione dell'efficacia della raccolta di **dati personali**, e come mezzo di successo per la gestione **di attività promozionali e di marketing**, per ricerche di mercato e per la profilazione degli utenti.

È quindi fondamentale conoscere le **regole** e le **best practice** per un loro uso corretto.

Hai mai provveduto alla creazione/integrazione delle Policy aziendali con una sezione dedicata appositamente alle procedure di utilizzo dei social network?

2. Gli ambiti regolamentari

Anche il fornitore di un servizio di social network deve conformare il suo funzionamento ai principi e alle **prescrizioni in materia di protezione dei dati**, applicando le misure necessarie per conformarsi alla normativa comunitaria.

In molti casi il fornitore di applicazioni riveste il ruolo di **Titolare del trattamento** dei dati, con i conseguenti obblighi nei confronti degli **utenti**, cominciando dalla necessità di garantire un'elevata sicurezza e un uso di impostazioni di **default** orientate alla Privacy come punto di partenza ideale per tutti i servizi proposti (ad es. limitare l'accesso alle informazioni del profilo-utente).

Inoltre, altre questioni da considerare sono il trattamento di **immagini** e di **dati sensibili**, così come la **pubblicità** e la commercializzazione diretta, la **conservazione** dei dati.

È necessario poi riservare particolare attenzione al trattamento dei dati personali dei **minori**.

Conosci gli account ufficiali aziendali sui social e come sono gestiti?

3. L'organizzazione interna per l'uso dei Social Media in azienda

La presenza del proprio marchio nei social network è fondamentale per garantire una coerente diffusione della propria brand image. Questo risultato può essere raggiunto solo coinvolgendo nel processo tutte le funzioni aziendali rilevanti. Si ritiene necessario il ricorso alla stesura di una **Policy** opportunamente dedicata all'utilizzo degli stessi o, in alternativa, in un paragrafo specifico inserito all'interno di altra Policy aziendale (es. Policy sull'utilizzo dei mezzi aziendali, posta elettronica ed internet).

In tale documento occorrerà, ad esempio, indicare i profili ufficiali dei social aziendali come gli

unici autorizzati a riflettere opinioni/posizioni della società ed il flusso di lavoro che abilita al controllo e pubblicazione sui social stessi, che dovrebbe passare al vaglio di un soggetto (Social Media Manager), alla quale faranno quindi riferimento tutti quegli incaricati o responsabili del trattamento autorizzati.

Come si pone la tua azienda nei confronti dell'uso degli account personali dei dipendenti sui social network?

Le procedure contenute in una Policy devono poi estendersi ai comportamenti da seguire in caso di incidenti che possano perturbare l'immagine, la reputazione e la sicurezza informatica aziendale nonché, nel caso di attività sospette concernenti i profili social aziendali.

A tal proposito, un caso realmente accaduto definibile come **cyber-bufala** e riferibile a una nota catena di abbigliamento femminile. I mega-sconti sul web erano una bufala, prima limitandosi alla vetrina di Instagram e poi al classico annuncio sul profilo Facebook (naturalmente falso) della catena. Quattrocentocinquanta fantomatici buoni shopping da 500 euro che hanno fatto cadere nella rete dei social network circa 20 mila persone compiendo in mezza giornata la presa in giro del mondo. Gli appassionati della moda "zerocost" hanno seguito con scrupolo le regole per accedere alla super offerta.
Le bacheche di Facebook e Twitter valgono oro e la possibilità di sfruttare un noto brand per **sottrarre dati personali** o comunque per guadagnare sfruttando i **banner pubblicitari** non è più una lontana realtà.
La non corretta **gestione Privacy** della pagina istituzionale dei **social network** può trasformarsi in un danno reputazionale (in caso di furto di identità e/o hacking della landing page), con possibili problemi derivanti dai cosiddetti "**data breach**" (violazione dei dati personali).

4. I Social Media e il Marketing

Un utilizzo consapevole dei social può altresì portare notevoli vantaggi dal punto di vista del marketing: non solo per far conoscere meglio il proprio brand ed essere più vicino ai propri (potenziali) clienti, ma anche per veicolare comunicazioni commerciali.
La pubblicazione delle **Linee guida in materia di attività promozionale e contrasto allo spam** rilasciate dal Garante per la protezione dei dati personali il 4 luglio del 2013, affrontano per la prima volta gli aspetti Privacy legati alle attività di marketing effettuate sui social media (fan page di Facebook et similia), fornendo importanti indicazioni operative.

Se non utilizzate correttamente, il rischio è il cosiddetto **Social Spam**, che consiste nell'invio di messaggi e link promozionali o di vendita diretta o per il compimento di ricerche di mercato attraverso le reti sociali on line effettuato senza l'autorizzazione da parte dei soggetti interessati.

L'enorme disponibilità dei dati personali in rete e la relativa facilità di raccolta degli stessi non è una valida autorizzazione per attività di inoltro di messaggi promozionali e per attività di analisi e profilazioni commerciali. Tali attività sono infatti disciplinate e sanzionate in caso di violazione dal Codice Privacy.

Il caso che il Garante Privacy considera lecito è quello riferibile ad un utente che decide di seguire i commenti, le opinioni, le novità e attività di un determinato personaggio e/o professionista, di una società, di uno specifico marchio o prodotto o servizio, diventando un "**follower**" e/o iscrivendosi anche ad uno specifico "**gruppo**" oppure un "**fan**" direttamente tramite la relativa pagina aziendale social. In virtù di tale adesione, l'utente riceve messaggi promozionali inerenti a quanto di suo interesse e come sopra indicato. In tale ipotesi, il trattamento potrà considerarsi lecito se dal relativo social network risulti in maniera chiara e

inequivocabile tali possibilità per le suindicate finalità e la stessa pagina aziendale social nel suo contesto fornisca delle informazioni in merito a tali attività promozionali.

Stai sfruttando tutte le possibilità di marketing che offrono i social network nel rispetto della normativa Privacy?

5. Conclusioni

I rischi che derivano da un uso non corretto dei Social Media sono rappresentati non solo dalle sanzioni che potrebbero scaturire da trattamenti con conformi alle normative vigenti in materia, ma anche da quelli di immagine e reputazionali.

Sì quindi all'uso dei Social Media nel rispetto delle regole, con la previsione di un aggiornamento delle **Privacy Policy aziendali** con inserimento di un capitolo in merito all'utilizzo dei social media da parte dei dipendenti e alla redazione di testi di **informative e consensi** ex D.lgs. 196/2003 in materia di protezione dei dati personali sui social media (fan page Facebook et similia come da Linee guida su marketing e spam del Garante).

Gli Autori

LUCA LEONE - Responsabile Servizi Privacy Sistemi Uno S.r.l.

- Privacy Officer e Consulente della Privacy - Schema TUV Italia 003_CDP – n°022
- Docente di corsi Formazione certificati secondo la normativa UNI EN ISO 9001: 2008 - EA 37
- Lead Auditor per Sistemi di Gestione Informatica e Telecomunicazioni (ISO 27001:2005)
- Implementer di Sistemi di Gestione Informatica e Telecomunicazioni (ISO 27001:2005).
- Lead Auditor per Sistemi di Gestione della Sicurezza dei Dati e delle Informazioni (BS 7799-2:2002 e ISO 19011:2002)

Cura i contenuti dei corsi di formazione in materia di Privacy del sistema FAD UnoLearning.it (www.unolearning.it) e la rubrica “Privacy” per Eutekne S.p.A.
Ha inoltre collaborato, in qualità di esperto, alla realizzazione di progetti nazionali come “PMI Internet” di Confindustria. E’ socio Fellow dell’Istituto Italiano per la Privacy.

ANTONIO SERRIELLO – Consulente Servizi Privacy Sistemi Uno S.r.l.

- Privacy Officer e Consulente Privacy - Schema TUV Italia 003_CDP - n° 028
- Docente di corsi Formazione certificati secondo la normativa UNI EN ISO 9001: 2008 - EA 37
- Implementer di Sistemi di Gestione Informatica e Telecomunicazioni (ISO 27001:2005)

Cura i contenuti dei corsi di formazione in materia di Privacy del sistema FAD UnoLearning.it (www.unolearning.it) e la rubrica “Privacy” per Eutekne S.p.A.

Unolegal

Unolegal è la Business Unit del Gruppo Sistemi UNO strutturata per fornire la consulenza legale e normativa in materia di Privacy. Essa nasce dall’incontro di competenze eterogenee: la competenza legale, la competenza tecnico-sistemistica e la competenza organizzativa. Unolegal realizza percorsi formativi verticalizzati sia per settore (banche, aziende sanitarie, studi professionali, imprese di produzione, commercio, servizi, P.A.) sia per argomento (Responsabili Privacy, Amministratori di Sistema, Marketing, Data Protection Officer).

Sei pronto ad affrontare un controllo del Garante Privacy?

Scopri gli argomenti dei nostri corsi per affrontare il controllo del Garante Privacy

http://corsi.unolegal.it