

# Le app per smartphone e tablet: gli adempimenti privacy

Dott. Valentino Spataro

Maggio 2014

documentazione: [www.garanteprivacy.it](http://www.garanteprivacy.it)

[www.iusondemand.eu/privacy-mobile](http://www.iusondemand.eu/privacy-mobile)



## Indice generale

Le app per smartphone e tablet:

gli adempimenti privacy

Introduzione

Le Autorità per la privacy europee adottano un parere sulle app

I rischi per la privacy delle applicazioni per smartphone

Obblighi e raccomandazioni

Il parere sulle app

4 Conclusions and recommendations

App developers must

The Working Party recommends that app developers

App stores must

OS and device manufacturers must

Third parties must

The Working Party recommends that third parties

Il Garante scrive a WhatsApp: come utilizzate i dati degli utenti italiani?

Privacy: Soro, app sempre più diffuse, servono garanzie

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

Attenzione ai dati conservati su smartphone e tablet

Proteggi i tuoi dati

Quando navighi su smarphone e tablet

APP-rova di privacy

Occhio allo spam

Vuoi sempre far sapere dove sei?

DICHIARAZIONE DI VARSAVIA sulla "appificazione" della società

Pagamenti via smartphone e tablet: le regole del Garante privacy per tutelare gli utenti. Avviata una consultazione pubblica

Informativa

Consenso

Misure di sicurezza

Conservazione

Consulenze

## Introduzione

E ora in molti si dispereranno.

Non avendo pensato prima agli aspetti della privacy, ora i costi di aggiornamento delle app saranno considerevoli.

Dalla parte degli sviluppatori mancano comunque linee guida di comportamento per sviluppare app conformi alle leggi italiane.

Il primo passo e' stato quello di **catalogare la documentazione in italiano e inglese gia' disponibile sul sito del Garante della Privacy o sul gruppo europeo art. 29.**

Questa e' la finalita' di questa raccolta.

Su [www.iusondemand.eu/privacy-mobile](http://www.iusondemand.eu/privacy-mobile) potete postare le vostre domande in materia.

Sara' nostra cura rispondere gratuitamente in termini generali in pubblico, e a pagamento per chi ha bisogno di una risposta specifica o di un controllo della propria app, su prezzi chiari.

Ricordo che il tema riguarda:

- le app integralmente native,
- parzialmente native,
- web app
- certi siti mobile / responsive o con librerie javascript e framework evoluti.

E' da notare che e' in consultazione pubblica un testo per la privacy nell'e-commerce mobile, ancora da approvare, ma gia' rilevante.

A tutti, buona consultazione.

Dott. Valentino Spataro

L'autore:

- **programma** computer dal 1986 in basic e assembler del 6502;
- e' stato **sysop** Fidonet negli anni 90;
- **sviluppa sul web** dal 1996 in perl e oggi in php, mysql, javascript, jquery, css, e gestisce server;

- si laurea in **giurisprudenza** del 1996;
- e' autore del sito **Civile.it** rivolto agli avvocati;
- ha realizzato il **dizionario legale** di internet, 1450 voci  
[www.civile.it/internet/dizionario.php](http://www.civile.it/internet/dizionario.php)
- ha sviluppato software per **cms, search engine, store, epayment, social network**;
- e' stato **praticante** avvocato fino al 2002;
- e' **amm.** di IusOnDemand srl dal 2003;
- sviluppa in html per mobile e sa **leggere il codice sorgente Objective C** (ma non sviluppa);
- conosce le **interfacce** utente ed il mondo **ios** e **firefox os**;
- **Nel 2014 ha vinto l'hackathon per l'Europa** a Londra sugli strumenti a tutela della privacy insieme al ricercatore di Reubin Binns dell'universita' di Southampton;

Per verificare, visitate l'home page di [www.IusOnDemand.eu](http://www.IusOnDemand.eu)

Questo garantisce una conoscenza del mercato, degli aspetti tecnici e degli aspetti legali. Da anni.

Su [www.iusondemand.eu/privacy-mobile](http://www.iusondemand.eu/privacy-mobile) potete postare tutte le domande in materia e trovare uno standard aperto per pubblicare i documenti legali.

Segue la raccolta di documenti ufficiali pubblicati dal sito del Garante,  
[www.garanteprivacy.it](http://www.garanteprivacy.it)

## Le Autorità per la privacy europee adottano un parere sulle app

Il consenso libero ed informato degli utenti finali è essenziale per garantire il rispetto della legislazione europea sulla protezione dei dati

Le Autorità europee per la protezione dei dati, riunite nel "Gruppo Articolo 29", hanno adottato un parere che esamina i rischi fondamentali per la protezione dei dati derivanti dalle applicazioni per terminali mobili. Nel parere sono indicati gli obblighi specifici che, in base alla legislazione Ue sulla privacy, sviluppatori, ma anche distributori e produttori di sistemi operativi e apparecchi di telefonia mobile, sono tenuti a rispettare. Particolare attenzione viene posta nel parere alle applicazioni rivolte ai minori.

Chi possiede uno smartphone ha normalmente attive in media circa 40 applicazioni. Queste applicazioni sono in grado di raccogliere grandi quantità di dati personali: ad esempio, accedendo alle raccolte di foto oppure utilizzando dati di localizzazione. "Spesso tutto ciò avviene senza che l'utente dia un consenso libero ed informato, quindi in violazione della legislazione europea sulla protezione dei dati" - afferma il Presidente dell'Autorità italiana per la privacy, Antonello Soro. "La nostra Autorità - continua Soro - ha dato un contributo significativo all'elaborazione del parere. Le app sono sempre più diffuse e il loro uso, senza un'adeguata definizione di garanzie e misure a tutela dei dati personali, può comportare rischi per gli utenti che le scaricano. Per questo è fondamentale muoversi in tempo".

### **I rischi per la privacy delle applicazioni per smartphone**

Gli smartphone e i tablet contengono grandi quantità di dati molto personali che riguardano direttamente o indirettamente gli utenti: indirizzi, dati sulla localizzazione geografica, informazioni bancarie, foto, video. Smartphone e tablet sono, inoltre, in grado di registrare o catturare in tempo reale varie tipologie di informazioni attraverso molteplici sensori quali microfoni, bussole o altri dispositivi utilizzati per tracciare gli spostamenti dell'utente. Anche se l'obiettivo degli sviluppatori è rendere disponibili servizi nuovi e innovativi, le app possono comportare rischi significativi per la privacy e la reputazione degli utenti.

La legislazione sulla privacy Ue prevede che ogni persona ha il diritto di decidere sui propri dati personali. Le applicazioni, dunque, per trattare i dati degli utenti devono prima fornire informative adeguate, in modo da ottenere un consenso che sia veramente libero e informato.

Un altro rischio per la protezione dei dati deriva da misure di sicurezza insufficienti. Insufficienza che può comportare trattamenti non autorizzati di dati personali a causa della tendenza a raccogliere quantità sempre più consistenti di informazioni e della elasticità e genericità degli scopi per i quali queste vengono raccolte, ad esempio a fini di "ricerche di mercato". Tutto ciò aumenta la possibilità di violazioni dei dati.

## **Obblighi e raccomandazioni**

Il parere individua precise raccomandazioni e obblighi per ciascuno degli attori coinvolti, evidenziando che la protezione di dati personali degli utenti e la relativa sicurezza sono il risultato di azioni coordinate di sviluppatori, produttori dei sistemi operativi e distributori ("app stores") che devono durare nel tempo, e non la semplice applicazione di regole una tantum. In particolare, sono richiamati gli obblighi sull'informativa e sul consenso riguardo all'archiviazione di informazioni sui terminali degli utenti, nonché per l'utilizzo da parte delle app di dati di localizzazione o delle rubriche dei contatti. Si raccomandano inoltre alcune "buone pratiche" che devono intervenire sin dalle fasi iniziali di sviluppo delle app, quali l'impiego di identificativi non persistenti, in modo da ridurre al minimo il rischio di tracciamenti degli utenti per tempi indefiniti, la definizione di precisi tempi di conservazione dei dati raccolti, l'impiego di icone "user friendly" per segnalare che specifici trattamenti di dati sono in corso (ad es. dati di geolocalizzazione).

In caso di app rivolte specificamente ai minori, si ribadisce la necessità del consenso dei genitori.

Si sottolinea, infine, la necessità di una più efficace assistenza all'utente mediante la designazione di "punti di contatto" presso gli "stores" che consentano agli utenti di risolvere in modo rapido problemi legati al trattamento di dati personali da parte delle app installate.

Roma, 14 marzo 2013

# Il parere sulle app

[WP202 Opinion 02/2013 on apps on smart devices.pdf \(816 k\)](#)

## 4 Conclusions and recommendations

Many types of data available on a smart mobile device are personal data. The relevant legal framework is the Data Protection Directive, in combination with the specific consent- requirement contained in Article 5(3) of the ePrivacy directive. These rules apply to any app targeted to app users within the EU, regardless of the location of the app developer or app store.

The fragmented nature of the app ecosystem, the wide range of technical access possibilities to data stored in or generated by mobile devices and the lack of legal awareness amongst developers create a number of serious data protection risks for app users. These risks range from a lack of transparency and lack of awareness amongst app users to poor security measures, invalid consent mechanisms, a trend towards data maximisation and elasticity of data processing purposes.

There is an overlap of data protection responsibilities between the different parties involved in the development, distribution and technical capabilities of apps. Most conclusions and recommendations are aimed at app developers (in that they have the greatest control over the precise manner in which the processing is undertaken or information presented within the app), but often, in order for them to achieve the highest standards of privacy and data protection, they have to collaborate with other parties in the app ecosystem, such as the OS and device manufacturers, the app stores and third parties, such as analytics providers and advertising networks.

### App developers must

- Be aware of, and comply with, their obligations as data controllers when they process data from and about users;
- Be aware of, and comply with, their obligations as data controllers when they contract with data processors such as if they outsource the collection and processing of personal data to developers, programmers and for example cloud storage providers;
- Ask for consent before the app starts to retrieve or place information on the device, i.e., before installation of the app. Such consent has to be freely given, specific

and informed;

- Ask for granular consent for each type of data the app will access; at least for the categories Location, Contacts, Unique Device Identifier, Identity of the data subject, Identity of the phone, Credit card and payment data, Telephony and SMS, Browsing history, Email, Social networks credentials and Biometrics;
- Be aware that consent does not legitimise excessive or disproportionate data

processing;

- Provide well-defined and comprehensible purposes of the data processing in advance to installation of the app, and not change these purposes without renewed consent; provide comprehensive information if the data will be used for third party purposes, such as advertising or analytics;

- Allow users to revoke their consent and uninstall the app, and delete data where appropriate;

- Respect the principle of data minimisation and only collect those data that are strictly necessary to perform the desired functionality;

- Take the necessary organisational and technical measures to ensure the protection of the personal data they process, at all stages of the design and implementation of the app (privacy by design), as defined in in section 3.6 of this Opinion;

- Provide a single point of contact for the users of the app;

- Provide a readable, understandable and easily accessible privacy policy, which at a minimum informs users about:

- who they are (identity and contact details),

- what precise categories of personal data the app wants to collect and process,

- why the data processing is necessary (for what precise purposes),

- whether data will be disclosed to third parties (not just a generic but a specific description to whom the data will be disclosed),

- what rights users have, in terms of withdrawal of consent and deletion of data;

Enable app users to exercise their rights of access, rectification, erasure and their right to

object to data processing and inform them about the existence of these mechanisms;

Define a reasonable retention period for data collected with the app and predefine a period

of inactivity after which the account will be treated as expired;

With regard to apps aimed at children: pay attention to the age limit defining children or minors in national legislation, choose the most restrictive data processing approach in full respect of the principles of data minimization and purpose limitation, refrain from processing children's data for behavioural advertising purposes, either directly or indirectly and refrain from collecting data through the children about their relatives and/or friends.

## **The Working Party recommends that app developers**

- Study the relevant guidelines with regard to specific security risks and measures;
- Proactively inform users about personal data breaches along the lines of the requirements of the ePrivacy Directive;
  - Inform users about their proportionality considerations for the types of data collected or accessed on the device, the retention periods of the data and the applied security measures;
  - Develop tools to enable users to customise retention periods for their personal data based on their specific preferences and contexts, rather than offering pre-defined retention terms;
  - Include information in their privacy policy dedicated to European users;
  - Develop and implement simple but secure online access tools for users, without collecting additional excessive personal data;
  - Together with the OS and device manufacturers and app stores use their creative talent to develop innovative solutions to adequately inform users on mobile devices, for example through a system of layered information notices combined with meaningful icons.

## **App stores must**

- Be aware of, and comply with, their obligations as data controllers when they process data from and about users;
    - Enforce the information obligation of the app developer, including the types of data the app is able to access and for what purposes, as well as whether the data is shared with third parties ;
    - Give special attention to apps directed at children to protect against the unlawful processing of their data, and especially enforce the obligation to present the relevant information in a simple manner, in age specific language;
    - Provide detailed information on the app submission checks they actually perform, including those aimed to assess privacy and data protection issues.
- The Working Party recommends that app stores
- In collaboration with the OS manufacturer, develop control tools for users, such as symbols representing access to data on and generated by the mobile device;
  - Subject all apps to a public reputation mechanism;

28•

Implement a privacy friendly remote uninstall mechanism;

Provide feedback channels to users to report privacy and/or security problems;

Collaborate with app developers to pro-actively inform users about personal data breaches;

Warn app developers about the specificities of European law before submitting the application in Europe, for example about the consent requirement and in case of

transfers

of personal data to non-EU countries.

### **OS and device manufacturers must**

- Update their APIs, store rules and user interfaces to offer users sufficient control to exercise valid consent over the data processed by apps;

- Implement consent collection mechanisms in their OS at the first launch of the app or the first time the app attempts to access one of the categories of data that have significant impact on privacy;

- Employ privacy by design principles to prevent secret monitoring of the user;

- Ensure security of processing;

- Ensure (the default settings of) pre-installed apps are compliant with European data protection law;

- Offer granular access to data, sensors and services, in order to ensure that the app developer can only access those data that are necessary for his app;

- Provide user-friendly and effective means to avoid being tracked by advertisers and any other third party. The default settings must be such as to avoid any tracking;

- Ensure the availability of appropriate mechanisms to inform and educate the end user about what the apps can do and what data they are able to access;

- Ensure that each access to a category of data is reflected in the information of the user before the app's installation : the categories presented must be clear and comprehensible;

- Implement a security-friendly environment, with tools to prevent malicious apps from spreading and allow each functionality to be installed/uninstalled easily.

The Working Party recommends that OS and device manufacturers

- Enable users to uninstall apps, and provide a signal (for example through the API) to the app developer to enable deletion of the relevant user data;

- Systematically offer and facilitate regular security updates;

- Ensure that methods and functions allowing access to personal data include features aiming to implement granular consent requests;

- Actively help develop and facilitate icons alerting users to different data usage by apps;

- Develop clear audit trails into the devices such that end users can clearly see which apps have been accessing data on their devices and the amounts of outgoing traffic per app, in relation to user-initiated traffic.

### **Third parties must**

- Be aware of, and comply with, their obligations as data controllers when they process personal data about users;

- Comply with the consent requirement determined in Article 5(3) of the ePrivacy

Directive when they read or write data on mobile devices, in cooperation with the app developers and/or app stores, which essentially provide user with the information on the purposes of data processing;

- Not circumvent any mechanism designed to avoid tracking, as it currently often happens with the "Do Not Track" mechanisms implemented in browsers;

29• Communications service providers, when they issue branded devices, must ensure the valid consent of users for pre-installed apps and take on board relevant responsibilities when contributing to determining certain features of the device and of the OS, e.g. when limiting the user's access to certain configuration parameters or filtering fix releases (security and functional ones) provided by the device and OS manufacturers;

Advertising parties must specifically avoid delivering ads outside the context of the app.

Examples are delivering ads by modifying browser settings or placing icons on the mobile desktop. Refrain from the use of unique device or subscriber identifiers for the purpose of tracking;

Refrain from processing children's data for behavioural advertising purposes, either directly or indirectly. Apply appropriate security measures. This includes secure transmission and encrypted storage of unique device and app user identifiers and other personal data.

### **The Working Party recommends that third parties**

- Develop and implement simple but secure online access tools for users, without collecting additional excessive personal data;

- Only collect and process data that are consistent with the context where the user provides the data.

## Il Garante scrive a WhatsApp: come utilizzate i dati degli utenti italiani?

Il Garante per la privacy ha chiesto alla società californiana che fornisce WhatsApp di comunicare ogni informazione utile per valutare il rispetto della privacy degli utenti italiani.

L'intervento dell'Autorità trae origine dagli esiti di un recente rapporto dei Garanti per la privacy canadesi e olandesi dal quale sono emerse alcune caratteristiche nel funzionamento dell'applicazione sviluppata dalla società che potrebbero comportare implicazioni e rischi specifici per la protezione dei dati personali degli utenti. Questi ultimi, infatti, per poter usufruire del servizio di messaggistica, devono consentire che l'applicazione acceda alla rubrica dei contatti presente sul proprio smartphone o sul proprio tablet e cioè a dati personali di soggetti terzi, anche però di coloro che non hanno scaricato l'applicazione e non utilizzano quindi il servizio. Nel rapporto sono state inoltre ipotizzate possibili criticità nelle misure di sicurezza adottate, in particolare riguardo alla conservazione dei dati trattati e al loro accesso da parte di terzi non autorizzati.

Il Garante ha dunque scritto a WhatsApp Inc. chiedendo di chiarire una serie di aspetti: quali tipi di dati personali degli utenti vengono raccolti e usati al momento dell'iscrizione e nel corso dell'erogazione dei servizi di messaggistica e condivisione file; come vengono conservati e protetti questi dati; le misure adottate (es. cifratura, generazione di credenziali etc.) per limitare il rischio di accesso da parte di soggetti diversi dagli interessati e, in particolare, se siano stati previsti sistemi contro gli attacchi tipo "man in the middle", volti ad acquisire illecitamente il contenuto dei messaggi scambiati mediante l'applicazione.

L'Autorità ha inoltre chiesto di sapere per quanto tempo vengono conservati i dati degli utenti e il numero degli account riferibili a quelli italiani.

Anche questo ultimo intervento dell'Autorità, al pari di altre iniziative adottate di recente, mira a garantire i diritti dei cittadini pur nell'ampio e complesso contesto di servizi ormai globalizzati.

Roma, 27 febbraio 2013

## Privacy: Soro, app sempre più diffuse, servono garanzie

Dichiarazione di Antonello Soro, Presidente del Garante per la protezione dei dati personali

"La nostra Autorità ha dato un contributo significativo all'elaborazione del parere adottato dei Garanti UE sull'uso delle 'app' per evitare i rischi per la protezione dei dati personali": A sottolinearlo è il presidente del Garante privacy italiano, Antonello Soro.

Chi possiede uno smartphone normalmente ha attive in media circa 40 applicazioni, in grado di raccogliere grandi quantità di dati personali, per esempio accedendo alle raccolte di foto oppure utilizzando dati di localizzazione. "Spesso tutto ciò - fa notare Soro - avviene senza che l'utente dia un consenso libero ed informato, quindi in violazione della legislazione europea sulla protezione dei dati". "Le app sono sempre più diffuse e il loro uso, senza un'adeguata definizione di garanzie e misure a tutela dei dati personali, può comportare rischi per gli utenti che le scaricano. Per questo - conclude - è fondamentale muoversi in tempo".

14 marzo 2013

## 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-tutorial 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 tue 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.

# DICHIARAZIONE DI VARSAVIA sulla "appificazione" della società

Varsavia (Polonia) – 24 settembre 2013

Le applicazioni per dispositivi mobili (app) sono ormai onnipresenti. Le troviamo negli smartphone e nei tablet, sulle auto, in casa e fuori casa: sono sempre più numerosi gli oggetti che dispongono di interfacce-utente connesse ad Internet. Ammontano ad oltre 6 milioni le app oggi disponibili nel settore pubblico e privato, ed è un numero che aumenta di oltre 30.000 unità al giorno. Le app facilitano e vivacizzano molte delle attività che svolgiamo giornalmente; allo stesso tempo, le app raccolgono anche una grande mole di informazioni personali. Tutto ciò permette un monitoraggio digitale permanente, mentre gli utenti spesso non ne hanno consapevolezza né ne conoscono i fini ultimi.

Spesso gli sviluppatori di app non conoscono le implicazioni associate alla loro attività in termini di privacy, né hanno familiarità con concetti quali protezione della privacy sin dalla progettazione ("privacy by design") e protezione della privacy di default ("privacy by default"). I sistemi operativi e le piattaforme app più diffusi permettono, in realtà, di configurare alcune impostazioni relative alla privacy, ma non consentono agli utenti di avere il pieno controllo dei propri dati personali verificando quali dati siano raccolti e per quali finalità.

Durante la 35ma Conferenza internazionale tenutasi il 23 ed il 24 settembre 2013 a Varsavia, i rappresentanti delle autorità per la protezione dei dati e la privacy hanno discusso della "appificazione" della società, delle sfide derivanti dall'utilizzazione crescente di applicazioni per dispositivi mobili e degli approcci possibili a tali sfide.

Vari studi e documenti pubblicati dai soggetti che si occupano di protezione dati negli ultimi anni offrono preziose indicazioni in tema di rapporti fra apps e privacy; si possono ricordare, in via non esaustiva, il "Parere su apps e dispositivi intelligenti" del Gruppo "Articolo 29" dell'UE, la "Guidance for Mobile App Developers" [Linee-guida per gli sviluppatori di applicazioni per dispositivi mobili] del Privacy Commissioner canadese, lo studio della Federal Trade Commission degli Usa su "Mobile Privacy Disclosures: Building Trust through Transparency" [Comunicazioni di dati personali e privacy nei dispositivi mobili: costruire fiducia attraverso la trasparenza], nonché il "Memorandum di Sopot" adottato dal "Gruppo di Berlino" (International Working Group on Data Protection in Telecommunications) nel 2012.

Le Autorità riunite nella Conferenza hanno espresso l'impegno inequivocabile affinché sia garantita agli utenti una migliore interazione in termini di privacy, ed intendono rivolgersi a vari soggetti pubblici e privati per richiamarli alle funzioni ed alle responsabilità rispettive.

E' fondamentale che gli utenti abbiano e continuino ad avere il controllo dei propri dati. Devono poter decidere quali informazioni condividere, con chi condividerle e per quali finalità. A questo scopo, devono disporre, anche all'interno delle app, di informazioni chiare e comprensibili sui dati raccolti, prima che abbia inizio la raccolta effettiva di tali dati. Gli utenti devono avere la possibilità di scegliere caso per caso se consentire l'accesso ad alcune specifiche informazioni, quali i dati sull'ubicazione o gli indirizzi in rubrica. Soprattutto, nella messa a punto delle app occorre ispirarsi al principio di minimizzazione delle sorprese: niente elementi nascosti, nessuna raccolta di informazioni effettuata in modo occulto e non verificabile.

Gli sviluppatori di app sono fra i motori della crescita dell'economia digitale e semplificano a tutti noi lo svolgimento delle attività quotidiane. Allo stesso tempo, devono garantire il rispetto delle norme di privacy e protezione dati esistenti nei vari Paesi del mondo. Per raggiungere tale obiettivo e contemporaneamente non incidere sull'esperienza dell'utente, occorre che si tenga conto dei requisiti di privacy fin dalle fasi iniziali di messa a punto di un'app. In tal modo, la privacy può apportare anche benefici in termini di competitività perché consente di accrescere la fiducia dell'utente. Gli sviluppatori devono stabilire con chiarezza quali informazioni siano necessarie per il funzionamento dell'app, e devono garantire che non siano raccolti dati personali ulteriori senza il consenso informato dell'utente. Ciò vale anche qualora uno sviluppatore ricorra a codici o plug-in forniti da terzi, ad esempio da reti di distribuzione pubblicitaria. Gli sviluppatori devono avere sempre contezza sia di ciò che offrono sia di ciò che chiedono ai propri utenti.

Non sono solo gli sviluppatori di app a dover farsi carico di alcune responsabilità in termini di privacy.

Ai fornitori di sistemi operativi competono specifiche responsabilità con riguardo alle rispettive piattaforme. E' vero che ciò sta avvenendo in misura crescente, perché questi fornitori offrono la possibilità di gestire in via generale le impostazioni di privacy sui dispositivi mobili. Tuttavia, tali impostazioni non hanno una granularità sufficiente a consentire il pieno controllo dell'utente su tutti gli aspetti significativi della raccolta di dati personali. Poiché i fornitori di piattaforme operative creano e gestiscono l'architettura entro cui le app sono utilizzabili, essi si trovano nella condizione ideale per garantire la protezione dei dati; sulle loro spalle pesa una particolare responsabilità nei confronti degli utenti. Da questo punto di vista, occorre

incoraggiare l'impegno assunto dalle aziende del settore di rispettare certificazioni di qualità in termini di privacy o altre forme di certificazione che comprendano una verifica della loro osservanza.

Anche se la responsabilità di tutelare la privacy degli utenti compete in primo luogo ai soggetti operanti nel settore delle app, le Autorità per la privacy e la protezione dei dati possono e devono sensibilizzare sul tema sia tutti coloro che operano nel settore delle app, sia gli utenti delle app e l'opinione pubblica in generale. E' opportuno, in particolare, instaurare un dialogo con i fornitori di sistemi operativi al fine di garantire che le rispettive piattaforme operino secondo i principi-cardine della protezione dati. Non vogliamo rovinare la festa agli utilizzatori di app, ma bisogna evitare ogni abuso dei dati personali. Se le attività volte a promuovere migliori prassi in termini di privacy si riveleranno non sufficientemente efficaci, le Autorità saranno pronte ad applicare le norme di legge nel quadro di un impegno globale a riaffermare il pieno controllo da parte dell'utente.

Le Autorità per la privacy e la protezione dei dati di tutti i Paesi del mondo intendono adoperarsi nei prossimi dodici mesi per migliorare sostanzialmente la privacy e la protezione dei dati in questo ambito, e intendono riesaminare la questione durante la 36ma Conferenza internazionale di Mauritius.

Wojciech Rafal Wiewiorowski Jacob Kohnstamm  
Generalny Inspektor Ochrony Danych Presidente del Comitato esecutivo  
Danych Osobowych della Conferenza internazionale

## Pagamenti via smartphone e tablet: le regole del Garante privacy per tutelare gli utenti. Avviata una consultazione pubblica

Informativa sull'uso dei dati, misure di sicurezza forti, conservazione a tempo

Chi usa smartphone e tablet per acquistare servizi, abbonarsi a quotidiani on line, comprare e-book, scaricare a pagamento film o giochi sarà più garantito. Arrivano le regole del Garante per proteggere la privacy degli utenti che, tramite il proprio credito telefonico, effettuano pagamenti a distanza avvalendosi del cosiddetto mobile remote payment.

L'uso di questa nuova forma di pagamento, che è destinata a raggiungere in breve tempo una notevole diffusione e che accentua i processi di smaterializzazione dei trasferimenti di denaro, comporta infatti il trattamento di numerose informazioni personali (numero telefonico, dati anagrafici, informazioni sulla tipologia del servizio o del prodotto digitale richiesto, il relativo importo, data e ora dell'acquisto), in alcuni casi anche di natura sensibile.

Obiettivo del provvedimento generale dell'Autorità, dunque, è quello di garantire in un mercato del pagamento sempre più dinamico, un trattamento sicuro delle informazioni che riguardano gli utenti e prevenire i rischi di un loro uso improprio.

Le direttive del Garante sono rivolte ai tre principali soggetti che offrono servizi di mobile payment: operatori di comunicazione elettronica, che forniscono ai clienti un servizio di pagamento elettronico tramite cellulare, o con l'uso di una carta prepagata oppure mediante un abbonamento telefonico; gli aggregatori (hub), che mettono a disposizione degli operatori tlc e internet e gestiscono la piattaforma tecnologica per l'offerta di prodotti e servizi digitali; i venditori (merchant), che offrono contenuti digitali e vendono servizi editoriali, prodotti multimediali, giochi, servizi destinati ad un pubblico adulto.

Ecco, in sintesi, gli adempimenti che dovranno adottare le tre categorie di operatori coinvolti.

## **Informativa**

I provider telefonici ed internet e i venditori dovranno informare gli utenti specificando quali dati personali utilizzano e per quali scopi. Per tale motivo dovranno rilasciare l'informativa al momento dell'acquisto della scheda prepagata o della sottoscrizione del contratto di abbonamento telefonico ed inserirla nell'apposito modulo predisposto per la portabilità del numero. Gli aggregatori, che operano per conto dell'operatore telefonico, potranno predisporre una apposita pagina con la quale fornire l'informativa e la richiesta del consenso al trattamento dei dati.

## **Consenso**

I provider telefonici e internet e gli aggregatori, che operano per conto di questi in veste di responsabili del trattamento, non dovranno richiedere il consenso per la fornitura del servizio di mobile payment.

Il consenso è invece obbligatorio, sia per gli operatori che per i venditori, nel caso vengano svolte attività di marketing, profilazione, o i dati vengano comunicati a terzi. Se i dati utilizzati sono sensibili, occorrerà richiedere uno specifico consenso.

## **Misure di sicurezza**

Operatori, aggregatori e venditori saranno tenuti ad adottare precise misure per garantire la confidenzialità dei dati, quali: sistemi di autenticazione forte per l'accesso ai dati da parte del personale addetto, e procedure di tracciamento degli accessi e delle operazioni effettuate; criteri di codificazione dei prodotti e servizi; forme di mascheramento dei dati mediante sistemi crittografici. Dovranno essere adottate misure per scongiurare i rischi di incrocio delle diverse tipologie di dati a disposizione dell'operatore telefonico (dati di traffico, sul consumo, relativi alla rete fissa, relativi alla fornitura di servizi etc.) ed evitare la profilazione incrociata dell'utenza basata su abitudini, gusti e preferenze. Da prevedere anche accorgimenti tecnici per disattivare servizi destinati ad un pubblico adulto.

## **Conservazione**

I dati degli utenti trattati dagli operatori, dagli aggregatori e venditori, ivi compresi gli sms di attivazione e disattivazione del servizio, dovranno essere cancellati dopo 6 mesi. L'indirizzo Ip dell'utente dovrà invece essere cancellato dal venditore una volta terminata la procedura di acquisto del contenuto digitale. Per la conservazione dei dati di traffico telefonico e telematico coinvolti nelle operazioni di mobile payment si dovranno rispettare i periodi di tempo previsti dal Codice privacy.

Prima del varo definitivo del provvedimento, l'Autorità ha deciso di sottoporre il testo a una consultazione pubblica: soggetti interessati, associazioni di categoria degli imprenditori e dei consumatori, università, centri di ricerca, potranno far pervenire contributi e osservazioni al Garante per posta o attraverso la casella di posta elettronica appositamente attivata: [consultazionemp@gpdp.it](mailto:consultazionemp@gpdp.it)

Roma, 3 gennaio 2014

## Consulenze

Per consulenze e controllo delle app, visita:

[www.iusondemand.eu/privacy-mobile](http://www.iusondemand.eu/privacy-mobile)

## Indice generale

Le app per smartphone e tablet:.....	1
gli adempimenti privacy.....	1
Introduzione.....	3
Le Autorità per la privacy europee adottano un parere sulle app.....	5
I rischi per la privacy delle applicazioni per smartphone.....	5
Obblighi e raccomandazioni.....	6
Il parere sulle app.....	7
4 Conclusions and recommendations .....	7
App developers must .....	7
The Working Party recommends that app developers .....	9
App stores must .....	9
OS and device manufacturers must .....	10
Third parties must .....	10
The Working Party recommends that third parties .....	11
Il Garante scrive a WhatsApp: come utilizzate i dati degli utenti italiani?.....	12
Privacy: Soro, app sempre più diffuse, servono garanzie.....	13
Le indicazioni del Garante per tutelare la tua privacy quando usi smartphone e tablet.....	14
Attenzione ai dati conservati su smartphone e tablet.....	14
Proteggi i tuoi dati.....	14
Quando navighi su smarthone e tablet.....	15
APP-rova di privacy.....	15
Occhio allo spam.....	15
Vuoi sempre far sapere dove sei?.....	16
DICHIARAZIONE DI VARSAVIA sulla "appificazione" della società.....	17
Pagamenti via smartphone e tablet: le regole del Garante privacy per tutelare gli utenti. Avviata una consultazione pubblica.....	20
Informativa.....	21
Consenso.....	21
Misure di sicurezza.....	21
Conservazione.....	21
Consulenze.....	23