Smartphone e tablet

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Smartphone e *tablet*: scenari attuali e prospettive operative

Schede di documentazione

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Francesco Pizzetti, *Presidente*
Giuseppe Chiaravalloti, *Vice Presidente*
Mauro Paissan, *Componente*
Giuseppe Fortunato, *Componente*

Daniele De Paoli, *Segretario generale*

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

Smartphone e tablet: scenari attuali e prospettive operative

PAGINA BIANCA

INDICE

1. Il contesto delle mobile apps

1.1. Smartphone e tablet

1.2. Le mobile apps e i market

1.3. Smartphone e sistemi tradizionali: cosa cambia

2. L'indagine conoscitiva

2.1. L'attività istruttoria

2.2. Riscontri pervenuti

3. Aspetti critici legati all'utilizzo degli smartphone

3.1. Rischi e minacce specifici

4. Come aumentare le garanzie per gli utenti

PAGINA BIANCA

1. IL CONTESTO DELLE MOBILE APPS

1.1. Smartphone e tablet

Uno *smartphone* (o cellulare intelligente o telefono *touch*, cioè sensibile al tocco) è un dispositivo portatile, alimentato a batteria, che coniuga le funzionalità di telefono cellulare con quelle di elaborazione e trasmissione dati tipiche del mondo dei personal computer; esso, inoltre, impiega sensori per la determinazione della posizione (GPS) e per l'acquisizione di altri elementi dell'ambiente circostante l'utente. Le componenti *hardware* generalmente presenti in dispositivi di questo tipo sono riassunte in *Tabella 1*, le caratteristiche funzionali e la tipologia di destinazione d'uso sono rappresentate in *Tabella 2*:

Componenti trasmissive	Sensori e dispositivi
Modulo telefonico	Schermo *touch* inferiore ai 5"
Wifi (rete senza fili)	Altoparlante e microfono integrati
Bluetooth (rete senza fili)	Fotocamera/videocamera digitale
Radio FM	Dispositivo di localizzazione (GPS)
	Bussola digitale e altri sensori
	Moduli di pagamento

Tabella 1. Smartphone: caratteristiche + hardware di massima

Nuove caratteristiche
Applicazioni con funzionalità di localizzazione
Riconoscimento vocale, facciale e di immagini
Social network con possibilità di rendere nota la posizione geografica degli utenti
L'utente generalmente acquisisce applicazioni utilizzando lo specifico *market* dedicato (*OviStore* per *Nokia*, *Apple Store* per *Apple*, *Android Market* per *Google*, *Windows Market Place* per *Microsoft*)
Possibilità di confusione tra dati di origine diversa (es. quelli contenuti nella rubrica per uso personale e quelli relativi ai contatti di lavoro.)

Tabella 2. Smartphone: applicazioni innovative e nuove funzionalità delle applicazioni tradizionali

I *tablet* o *tablet computer* sono dispositivi assimilabili per componenti *hardware* e *software* agli *smartphone*, dai quali si distinguono per:

- dimensioni dello schermo
- possibile assenza del modulo telefonico
- destinazione d'uso

Gli *smartphone* e i *tablet computer* per lo più condividono la stessa infrastruttura tecnologica ovvero le stesse componenti *hardware* e lo stesso sistema operativo. I *tablet* sono però caratterizzati da uno schermo di dimensioni maggiori, il che li rende più idonei al consumo di prodotti multimediali ed editoriali (es. *gaming on-line*, *film on-demand*, abbonamenti a riviste e quotidiani) e meno pratici per essere utilizzati come telefoni e come PIM (*Personal Information Management*); per questa ragione alcuni esemplari non sono dotati di modulo telefonico. La maggior parte dei modelli si avvale, tuttavia, di schede SIM per la connessione dati con le tecnologie cellulari (GPRS e UMTS).

È opportuno osservare che, per le finalità connesse alle problematiche relative alla protezione dei dati personali, sia i dispositivi *tablet* che *smartphone* possono essere considerati unitariamente, dal momento che le modalità di funzionamento delle applicazioni sono pressoché identiche. Va altresì evidenziato che non costituisce oggetto di indagine l'impiego di questi dispositivi come apparecchi telefonici per le comunicazioni interpersonali.

1.2. Le mobile apps e i market

Per *mobile apps* o applicazioni per *smartphone* si intende il *software* che è possibile installare sugli *smartphone* e sui *tablet* per fornire funzionalità aggiuntive. Le applicazioni per *smartphone* estendono, cioè, le funzionalità rese disponibili dal sistema operativo dello specifico produttore e sono reperibili tramite *download* da una speciale applicazione che acquisisce il marchio (*brand*) del produttore del telefono o del sistema operativo installato sul telefono. Tale particolare applicazione viene

detta *market* ed è denominata diversamente dai vari produttori. I principali *market* attualmente sono:

- *Android Market* (*Google*)
- *Apple Store* (*Apple*)
- *Windows MarketPlace* (*Microsoft*)
- *Nokia Ovistore* (*Nokia*)

Tutti i *market* sono una speciale applicazione per *smartphone* che visualizza una vetrina virtuale dalla quale è possibile acquisire ulteriori applicazioni.

1.3. Smartphone e sistemi tradizionali: cosa cambia

Tablet e *smartphone* si differenziano dai *netbook* e dai *notebook* più tradizionali non soltanto per la specificità dell'*hardware* e del *software* di base, ma anche e soprattutto per i meccanismi e le modalità di acquisizione e distribuzione del *software* (*software acquisition* & *distribution*), che sono centralizzati e normalmente controllati dal fornitore del dispositivo, dall'operatore telefonico, dal produttore del sistema operativo o, infine, dal *"gestore del market"* che opera da intermediario tra il produttore/sviluppatore dei software e dei servizi (nella maggior parte dei casi esterno alla società e, dunque, terzo rispetto ad essa) e l'utente finale. Infatti, con specifico riguardo a *smartphone* e *tablet*, l'utente acquista *software* aggiuntivi (es. un videogame) e servizi (es. un cruscotto dell'andamento titoli, un servizio di condizioni meteo, un film in *streaming*, un *videogame* in *multiplayer*) avvalendosi di un'applicazione fornita dal gestore denominata *market* e preinstallata sul dispositivo.

Come sopra accennato, si tratta di una sorta di vetrina dei *software* e dei servizi disponibili resa accessibile all'utente per ampliare le funzionalità *software* del proprio *smartphone*. Il relativo utilizzo richiede la preventiva registrazione dell'utente e l'accettazione, da parte di quest'ultimo, delle condizioni contrattuali prefissate dal gestore del *market*, cristallizzate in un documento denominato *terms of service* (*ToS*).

In linea di massima non è possibile acquisire un'applicazione tramite canali tradizionali (es. CD acquistato in negozio), né avvalersi di modalità alternative a quelle

rigidamente previste dal gestore dello specifico *market* di riferimento, che va considerato lo strumento privilegiato e più diffuso per la distribuzione e l'acquisizione delle applicazioni per *smartphone*. L'eventuale installazione di applicazioni al di fuori del *market* è da ritenersi, dunque, una possibilità residuale.

Parallelamente, anche uno sviluppatore terzo che intenda creare un'applicazione in ambito *mobile* sarà tenuto ad accettare i *ToS* definiti dal detentore della piattaforma da lui scelta, ovvero dal gestore del *market*, e potrà vendere il suo prodotto solo attraverso il canale previsto da quest'ultimo.

Va sottolineato che il panorama delle *mobile apps* è molto vivace e in rapida evoluzione, anche in considerazione del fatto che le tecnologie alla base delle *mobile apps* (quali l'introduzione dei citati sensori sugli *smartphone*, la nuova modalità *touch* di interfacciamento con lo strumento), la facilità di accesso e di utilizzo di questi dispositivi e le innovative modalità di distribuzione dei relativi servizi hanno aperto la via a nuove, concrete opportunità di *business*, all'implementazione tecnologica ed alla diffusione di servizi ed applicazioni del tutto impensabili solo fino a qualche tempo fa. Attualmente esistono numerosissimi sviluppatori in ogni parte del mondo, caratterizzati da dimensioni imprenditoriali anche molto limitate, a volte semplici appassionati individuali senza particolari ambizioni commerciali, i quali con bassissimi investimenti e puntando su un'idea o un'intuizione creano e, attraverso la vetrina resa disponibile dal gestore (il *market*), mettono a disposizione di un mercato potenzialmente mondiale soluzioni talvolta molto innovative, in genere dal costo anche molto contenuto, che l'utente può acquistare in tutta semplicità, autonomia ed immediatezza. È tuttavia presumibile che questa dimensione artigianale con il tempo tenderà ad evolversi, convergendo verso una contrazione del numero degli sviluppatori che assumeranno connotazioni di maggior strutturazione e di più ampie dimensioni: è, infatti, verosimile che le aspettative dei consumatori siano destinate a crescere, con l'effetto che i prodotti, per essere competitivi, dovranno essere progressivamente più complessi e diversificati, con conseguente aumento dei costi di ideazione e sviluppo.

2. L'INDAGINE CONOSCITIVA

2.1. L'attività istruttoria

Agli inizi del 2011 l'Autorità ha avviato un'indagine che ha avuto come interlocutori privilegiati i principali produttori di sistemi operativi per *smartphone* (nello specifico, *Nokia*, *Microsoft*, *Apple*, *Google*), al fine di verificare gli accorgimenti adottati da queste società per garantire la sicurezza nell'utilizzo delle *mobile apps* sviluppate per i loro sistemi.

In particolare, le società sono state invitate ad indicare:

1. i meccanismi adottati o i requisiti richiesti (in termini, ad esempio, di affidabilità o di adeguato rispetto di misure di sicurezza) per selezionare preventivamente gli sviluppatori terzi (quelli, cioè, non direttamente dipendenti dalla società) autorizzati a distribuire le *application* di propria creazione sulle piattaforme di *market* di quest'ultima e quali condizioni e procedure siano previste per un'eventuale revoca dell'autorizzazione;

2. i meccanismi adottati per valutare le diverse funzionalità delle *application* e per verificare se la raccolta di dati personali effettuata dallo sviluppatore, per il tramite dell'applicazione, sia effettivamente pertinente rispetto alle predette funzionalità e alle finalità della raccolta;

3. le *policies* interne per assicurare il rispetto della normativa in materia di protezione dei dati personali e quali meccanismi siano adottati per verificare la conformità delle *application* già distribuite alla predetta normativa, nel caso in cui pervengano segnalazioni da parte degli utenti.

2.2. Riscontri pervenuti

Le risposte rese dai soggetti interpellati hanno evidenziato l'adozione di politiche aziendali solo in parte comuni.

In tutti e quattro i casi oggetto di indagine, ad esempio, lo sviluppatore terzo può proporre le applicazioni di propria creazione per la distribuzione sulla piattaforma di *market* dell'intermediario prescelto soltanto a seguito del perfezionamento di una

procedura di registrazione ed all'accettazione di specifici accordi contrattuali predisposti, proprio, da quest'ultimo; ne consegue una marcata eterogeneità delle clausole contrattuali cui gli sviluppatori sono vincolati, a seconda che decidano di proporre le proprie creazioni all'una o all'altra delle quattro diverse società.

Le indicazioni fornite, segnate naturalmente dal carattere della confidenzialità, hanno evidenziato differenze più o meno sensibili anche in ordine alle attività di controllo, alle assunzioni di responsabilità, ai rimedi esperibili in caso di inconvenienti, sia di carattere tecnico, nel funzionamento dell'applicazione, sia di carattere giuridico e dunque maggiormente attinenti agli aspetti contrattuali.

Ulteriori diversità sono state osservate anche con specifico riguardo al profilo che più direttamente interessa questa Autorità, quello cioè della protezione dei dati personali degli utenti. In quest'ambito è stato possibile, tuttavia, identificare due diversi e contrapposti modelli di condotta, che si distinguono per il modo in cui viene garantita la sicurezza delle applicazioni messe in vendita tramite il *market* e possono essere definiti nel modo seguente:

- *privacy by process*
- *privacy by platform*

Nel modello *privacy by process*, il processo di accreditamento dei potenziali sviluppatori e di inserimento delle loro applicazioni nel *market* viene sottoposto ad un rigido controllo, tipicamente formalizzato in un accordo *ToS* (*Terms of Service* - condizioni di contratto) tra il soggetto interessato a pubblicare il suo *software* sul *market* e il gestore del *market* stesso. Inoltre, l'applicazione viene controllata allo scopo di garantirne la sicurezza sotto il profilo tecnico prima dell'immissione nel mercato.

Nel modello *privacy by platform* il gestore del *market* non effettua un controllo preventivo sull'applicazione, ma affida la tutela dei diritti dell'utente alla solidità della piattaforma di sistema operativo, alle sue funzionalità che permettono all'utente di avere coscienza di quali dati saranno oggetto di trattamento da parte dell'applicazione disponibile sul *market*, facendo ricorso a meccanismi di *ranking* gestiti dagli

stessi utenti. In termini più concreti, chi utilizza il *market* può verificare per ogni applicazione disponibile le opinioni di coloro che prima di lui ne hanno già fatto uso, espresse sotto forma di punteggi sintetici e commenti. Inoltre, all'atto dell'installazione di un'applicazione la piattaforma *software* presente sul suo *smartphone* provvede ad informare l'utente su quali funzionalità l'applicazione utilizzerà e quindi a quali dati può potenzialmente accedere.

3. ASPETTI CRITICI LEGATI ALL'UTILIZZO DEGLI *SMARTPHONE*

La diffusione dei moderni *smartphone* determina una crescita sostenuta nell'utilizzo delle applicazioni per questo tipo di dispositivi: i principali *market* hanno ormai un *portfolio* che può superare le decine di migliaia di *apps*.

Gli utenti tendono a delegare la gestione di molti aspetti della propria vita sia personale che professionale alle nuove tecnologie, le quali fanno sempre più spesso impiego di informazioni relative alla geolocalizzazione degli interessati. Questi dati non sempre restano archiviati esclusivamente sul dispositivo, ma vengono frequentemente conservati in aree remote potenzialmente accessibili anche da altri utenti. Uno stesso *smartphone* può essere utilizzato per le finalità più disparate, ad esempio per la gestione del *portfolio* clienti, del catalogo e del calendario aziendali, ma anche per la condivisione di foto, informazioni, video etc. con i propri amici o familiari, per il confronto dei prezzi dei prodotti al supermercato con quelli del negozio *on-line*, per monitorare i propri movimenti bancari, per localizzare la propria autovettura in caso si dimentichi dove è stata posteggiata, per sapere, in quel determinato momento, chi dei propri amici si trovi in zona, per redigere programmi di benessere alla stregua delle proprie abitudini alimentari, per impostare il monitoraggio ormonale del ciclo femminile, e magari, in una prospettiva di prossima, futura realizzazione, persino come telecomando per aprire il cancello automatico del proprio box auto o per sbloccare la serratura della propria abitazione. Il ventaglio delle applicazioni possibili è, allora, realmente impressionante e destinato

ad accrescersi ulteriormente. Tuttavia, l'utilizzo di tali applicazioni implica l'elaborazione e quindi il trattamento di dati, anche personali, riservati e persino sensibili. In molti casi i dati verranno archiviati e conservati sul dispositivo, ma sempre più spesso ci si avvale di *mobile apps* che consistono in realtà in servizi erogati in modalità *web*, il cui utilizzo implica, cioè, che le informazioni personali siano spostate o copiate nella *cloud* del fornitore del servizio. Il fornitore, ovvero lo sviluppatore delle *mobile apps*, può essere lo stesso gestore del *market* o uno sviluppatore indipendente. In altri termini, molte delle applicazioni per *smartphone* sono servizi erogati in modalità *cloud* (*"Saas" - Software as a service*) che trasportano tutti o parte dei dati dell'utente nella *cloud*.

La transizione dal modello applicativo tradizionale a quello in cui il *software* è un servizio della *cloud* è condivisa sia dal fornitore sia dal consumatore, in quanto la modalità *cloud* costituisce apparentemente un'esclusiva facilitazione per l'utente. In realtà questi non è, spesso, neppure consapevole del fatto che sta utilizzando un servizio *cloud*; è, tuttavia, perfettamente al corrente della possibilità di accedere agli stessi dati da dispositivi differenti (*es. smartphone* e pc da scrivania) ovvero che se acquista uno *smartphone* nuovo può ritrovare, *"come per magia"*, tutti i propri dati sul nuovo dispositivo senza dover ricorrere a tediose transizioni dal vecchio al nuovo telefonino (si pensi allo spostamento dei contatti della rubrica).

Un ulteriore aspetto che viene proposto e percepito come facilitazione a valore aggiunto è l'integrazione di *set* di dati che hanno origini differenti. Ad esempio con i telefoni basati sul *software* di *Google* (*Android*) è possibile trasferire nella rubrica dello *smartphone* i contatti, compresi quelli di posta elettronica, prelevati dall'*account* Google. Inoltre alcuni produttori di telefoni danno la possibilità all'utente di integrare tale rubrica con ulteriori dati prelevati dal proprio *account Facebook*, aggiungendo ad esempio le foto e gli indirizzi di residenza.

Questi, in sintesi, gli aspetti critici di carattere generale in merito all'utilizzo della nuova generazione dei dispositivi *smartphone*:

• sono dispositivi pervasivi, utilizzabili in tutti gli aspetti della vita personale e professionale;

• è presumibile che vi si farà sempre più frequentemente ricorso per gestire anche dati "riservati";

• le facilitazioni d'uso favoriscono l'esternalizzazione dei dati;

• le facilitazioni d'uso favoriscono l'integrazione di dati tra aspetti distinti della propria vita (es. rubrica lavorativa e amici su *Facebook*).

3.1. Rischi e minacce specifici

Le precedenti osservazioni consentono, allora, di definire, elencandoli, i principali fattori connessi all'utilizzo dei sistemi *mobile* idonei a determinare rischi e minacce specifici per la protezione dei dati personali degli utenti. Segnatamente:

• la linea di demarcazione che permette di distinguere l'*Identità digitale* dall'*Identità reale* tende progressivamente ad affievolirsi sino a scomparire. L'utilizzatore di *applications* per *smartphone* è, infatti, identificabile abbastanza facilmente attraverso informazioni obiettive e concrete, non autonomamente modificabili (ad esempio il numero di telefonino, il codice IMEI, i dati anagrafici dei contatti registrati nella rubrica archiviata sul proprio dispositivo etc.);

• il *social networking* tende ad essere sempre più pervasivo e si integra e arricchisce con nuove informazioni personali (ad esempio la posizione geografica dell'utente);

• in generale, a causa dell'integrazione dei servizi informatici e dello scambio di dati tra applicazioni, telefono e servizi, è sempre più difficile - e spesso impossibile - controllare il flusso dei propri dati personali;

• a causa della progressiva diminuzione del controllo sui propri dati e della correlata fusione tra l'identità digitale e quella reale, emergono maggiori pericoli dal punto di vista della sicurezza informatica e si creano nuovi rischi e minacce

(es. *stalking* sociale, intercettazioni, furto di *account* di pagamento);

• possibilità di accedere da parte delle applicazioni a dati e strumenti in un modo ancor più invasivo che in passato (numero di telefono, rubrica, messaggi);

• possibilità da parte delle applicazioni di intrecciare aspetti differenti della vita degli utenti (es. vita privata e vita professionale) in modi non sempre chiari, conoscibili, prevedibili, controllabili e desiderati da parte dell'utente stesso;

• tracciamento e profilazione dell'utente a sua insaputa e disponibilità di dati univoci (IMEI, numero di telefono) da utilizzare ad esempio per la pubblicità comportamentale, per l'enforcement di un accordo di servizio o per la tutela del diritto d'autore;

• alcuni produttori, per ragioni di mercato, tendono a non distribuire tempestivamente gli aggiornamenti *software* che risolvono accertate vulnerabilità di sicurezza informatica.

In un tentativo di ulteriore schematizzazione, i rischi e le minacce in cui un utente può incorrere per un uso non accorto o non regolamentato delle *mobile apps* derivano da:

• mancanza di TRASPARENZA nelle modalità e nelle finalità di raccolta dei dati;

• incapacità o impossibilità da parte degli interessati di esercitare o recuperare il CONTROLLO sui propri dati e sul modo in cui essi vengono comunicati a terzi;

• elementi tecnici di SICUREZZA INFORMATICA

Trasparenza	Controllo	Sicurezza informatica

Tabella 3: Le tre dimensioni della protezione dei dati personali nelle apps

4. COME AUMENTARE LE GARANZIE PER GLI UTENTI

In questa sede si intendono formulare proposte di carattere operativo tese a favorire sia l'utilizzo consapevole, da parte dell'utente, degli strumenti e dei dispositivi dei quali si tratta, sia un più efficace esercizio dei propri diritti in merito alla gestione dei dati personali.

È opportuno muovere da una duplice considerazione:

- i produttori di dispositivi e dei relativi *software*, così come gli operatori di telefonia che commercializzano tali dispositivi previa apposizione del proprio marchio (*brand*), rivestono un ruolo importante sul livello di sicurezza dei dispositivi *mobile* che distribuiscono; coerentemente, sono loro i soggetti deputati a garantire anche la messa a disposizione di aggiornamenti tempestivi qualora siano rilevate nuove minacce per la sicurezza informatica. A questo riguardo, giova specificare che le caratteristiche del sistema operativo associato ad uno specifico dispositivo mutano a seconda che l'operatore di telefonia vi abbia apposto il proprio *brand* oppure no e sono, dunque, soggette ad una sorta di "personalizzazione" legata, proprio, al *brand*. In termini più concreti, la configurazione del *software* di un dispositivo destinato ad essere commercializzato previa apposizione di un marchio (per esempio *Telecom Italia*, *Vodafone*, *Wind*, *H3G* etc.) è almeno in parte determinata dall'operatore di telefonia stesso, con l'obiettivo di renderne l'utilizzo il più possibile idoneo alla fruizione dei servizi che esso stesso mette a disposizione dei propri clienti. Ne consegue che due telefonini originariamente ed apparentemente identici, poiché dello stesso modello e della stessa marca, potranno in realtà differenziarsi in maniera anche significativa sotto il profilo delle caratteristiche del *software* a seconda del gestore che ne curi la personalizzazione e vi apponga il proprio *brand*. In questa ipotesi, le mutate caratteristiche del *software* di un dispositivo cui sia stato apposto il marchio dell'operatore di telefonia potrebbero, in alcuni casi, influire sul processo di aggiornamento del *software* reso disponibile dal produttore del telefonino (ad

esempio *Nokia*, *Sony Ericsson*, *Samsung*, *LG* etc.), rendendolo non direttamente ed immediatamente fruibile;

- nel caso delle *mobile apps*, a differenza del tradizionale modello di acquisizione del *software* su PC, c'è generalmente - lo si ribadisce - un intermediario univoco che si frappone tra lo sviluppatore / fornitore del servizio e l'utente finale; in altri termini, l'indeterminata molteplicità degli sviluppatori da un lato e l'altrettanto enorme massa degli utenti dall'altro trovano il loro punto di contatto e di raccordo proprio per il tramite di pochi soggetti, appunto gli intermediari, sulle cui attività imprenditoriali e commerciali si concentra il funzionamento del peculiare mercato di riferimento.

Il panorama prevalente consente, allora, di ipotizzare interventi mirati che, sfruttando la posizione di centralità degli intermediari all'interno della richiamata dialettica contrattuale e di *business*, possano efficacemente raggiungere la maggior parte dei soggetti coinvolti, con il dichiarato intento di porre le basi di una disciplina chiara ed efficace di tutela degli utenti in materia di protezione dei dati personali che non costituisca, tuttavia, un limite né dal punto di vista della logica concorrenziale propria del mercato né tantomeno abbia l'effetto di imbrigliare le potenzialità creative degli sviluppatori delle più moderne tecnologie.

In questa prospettiva, giova sottolineare che proprio all'intermediario, cioè al gestore del *market* che è spesso anche il produttore del sistema operativo dello *smartphone*, compete sempre un potere definitivo segnato dal massimo carattere della deterrenza, e cioè quello di interdizione nei confronti del *software* prodotto da terze parti con le quali sussista un vincolo di carattere contrattuale.

Una prima conclusione: è indispensabile, perché gli utenti siano posti nella condizione di decidere con responsabilità in ordine all'utilizzo dei propri dati, agire in modo da accrescerne la consapevolezza sulle opportunità, ma anche sui potenziali rischi riconducibili al mondo degli *smartphone* e delle *mobile apps*.

È altrettanto fondamentale che gli utenti, dopo aver conferito e, in senso lato, affidato i propri dati, ne mantengano comunque il controllo.