7 giugno 2011 11:14

Utenti IPhone e IPad: rischio privacy

di Deborah Bianchi *

Un database di circa 75 milioni di utenti iPhone, ciascuno identificato dal codice seriale del proprio melafonino (UDID). Ma soprattutto, molti dei quali collegati al proprio account Facebook, in modo che dal codice dello smartphone, virtualmente anonimo, sia possibile risalire all'identità del suo proprietario.
Tutto questo a disposizione di un singolo sviluppatore di applicazioni ma, per un lungo periodo di tempo, accessibile a chiunque via Internet.
Il nuovo rischio privacy per gli utenti iPhone (e iPad) ha un nome piuttosto tecnico, oltre che oscuro: "deanonimizzazione dell'UDID".
Per spiegarlo, in realtà, basta una domanda: cosa succederebbe se uno sviluppatore iPhone, o una delle società che intercettano i dati di utilizzo delle app, potesse identificare gli utenti che usano le applicazioni, creando un database con i dati personali di ciascuno?
Questo l'inquietante interrogativo che viene dalle colonne digitali di Repubblica, 3 giugno 2011.

Il dato elettronico, rivelando le attitudini di consumo e personali del netizen che lo ha messo in circolazione, costituisce oggi vero oggetto di diritti e di doveri.
Il Codice Privacy si fonda sul diritto al corretto trattamento del dato personale che nell'internet diventa diritto al corretto trattamento del dato elettronico.

La data protection si traduce *nel diritto a mantenere il controllo sulla circolazione del proprio patrimonio informativo digitale in modo che agenti esterni possano raccoglierlo e trattarlo solo previo consenso dell'interessato.*
Il patrimonio informativo elettronico del netizen, interfacciandosi con le piattaforme intelligenti (ad esempio ricerca su Google oppure costruzione del proprio profilo su Facebook) rilascia dati di contenuto (opinioni e gusti dell'utente espressi in rete) e dati tecnici inerenti al tipo e alle preferenze di navigazione (ad esempio in modalità totalmente aperta all'area web oppure con restrizioni sui cookies o su altri download che tenderebbero a installarsi in automatico).

I dati di contenuto e i dati tecnici tracciati durante il transito costruiscono l'identità informativa del soggetto in determinati spazi elettronici.

Quando parliamo di privacy in internet occorre avere la consapevolezza che nel mondo elettronico circolano due tipi di dati personali: i dati visibili e i dati invisibili.

I dati visibili sono quelli che attengono alle informazioni relative alla nostra persona, che si colgono nei file di testo (ad esempio un profilo Facebook in cui è reso pubblico il nostro indirizzo email), in un file di immagine (una foto), in un file audio-video (una ripresa video). Soprattutto nei social network attraverso la cosiddetta tecnica di "taggare", i dati sfuggono al controllo dell'interessato perché essendo implementati nel profilo di terze persone, amici degli amici degli amici, finiscono per circolare nella rete a prescindere dalla nostra volontà.

I dati invisibili sono quelli che vengono prodotti dai software che servono per la navigazione in internet. Ogni volta che il nostro pc si collega ad internet rilascia al server del fornitore di connettività (ad esempio Telecom) indicazioni che registrano la data e l'ora del collegamento (i cosìddetti file di log); indicazioni sui siti frequentati (tracciabilità del percorso elettronico intrapreso); indicazioni sul tempo trascorso in un determinato sito piuttosto che in un altro (tracciabilità dei gusti del navigatore). Mentre navighiamo senza accorgercene lasciamo impronte telematiche in tutti i luoghi frequentati e questo consente di ricostruire un profilo abbastanza fedele delle nostre preferenze e dei nostri interessi.

Il dato personale (visibile o invisibile) in internet è diventato un affare da migliaia di euro. Gli operatori di marketing o di pubblicità ambiscono ad avere i profili delle nostre preferenze derivati dai tracciati dei nostri viaggi telematici, perché così riescono a piazzare il prodotto o il servizio in un mercato che sicuramente si è dimostrato potenzialmente sensibile a questo tipo di merce.

Da qui gli esempi di attentati quotidiani alla sicurezza dei nostri dati in internet. Pensiamo ai cookies: si tratta di software che si installano sul pc dell'utente al momento della richiesta di connessione a un determinato sito web. Di conseguenza il sito web che ha piazzato il cookie nel nostro pc ogni volta che frequentiamo quella pagina elettronica è in grado di spiare le nostre mosse. Ovviamente tutto questo avviene in violazione della nostra privacy.

Per gli utenti Apple di Iphone e Ipad c'è l'ulteriore rischio evidenziato sopra.
Le applicazioni utilizzate da quel determinato dispositivo mobile che si abbina a quel certo nominativo rivelano i gusti e le preferenze ovvero i mercati a cui quel soggetto può essere sensibile.

Scandalizzati?

No, non credo. L'importante è essere consapevoli dei fenomeni. E' chiaro che l'internet si regge su queste logiche di mercato altrimenti non potrebbe trovare le risorse per svilupparsi. Il dato è la fonte economica maggiore della web economy. Di conseguenza occorre sempre ragionare in un'ottica di bilanciamento degli interessi sacrificando un po' dell'uno e un po' dell'altro a seconda delle circostanze.

Così nel caso di Apple occorrerà trovare una misura adeguata per il sacrificio della privacy dell'utente.
Ad esempio potremo pensare che gli utenti che decidono volontariamente e consapevolmente di svelare un po' di sé in Rete avranno accesso a certe applicazioni gratuitamente mentre gli utenti che vogliono rimanere riservati dovranno pagare integralmente quelle stesse applicazioni.

Il nucleo centrale della questione è l'informativa al soggetto in modo da renderlo in grado di essere sempre sovrano del proprio patrimonio informativo.

**** Deborah Bianchi,*** *avvocato specializzato in diritto applicato alle nuove tecnologie, esercita nel Foro di Pistoia e Firenze in materia civile e amministrativa avv.deborah(at)deborahbianchi.it*