TECNOLOGIE PER LA SICUREZZA E PRIVATEZZA – a.a. 2012/2013

TECNOLOGIA E LEGISLAZIONE

Salvatore Fresta

Garantire la **privatezza dei dati** significa mettere in atto dei meccanismi che siano in grado di:

- fornire la **protezione della privatezza**, quindi dei meccanismi che siano in grado da una parte di rilasciare informazioni senza che sia possibile individuare **proprietà specifiche** delle entità coinvolte (dove per entità si può intendere un utente o un'organizzazione) e dell'altra **limitare le informazioni** che possono essere acquisite.

- evitare il **data linkage** (**collegamento dei dati**), ovvero evitare che combinazioni di dati provenienti da **fonti diverse** (ad esempio i vari medici che si occupano dello stesso paziente) forniscano informazioni sull'entità.

Per garantire la privatezza dei dati non bisogna considerare solo gli **aspetti tecnologici** bensì anche quelli **legali** (le problematiche di privatezza devono essere regolamentate anche a livello legislativo) ed **economici** (le problematiche di sicurezza non sempre hanno una diretta interpretazione economica).

I **gestori di siti web** raccolgono molto spesso informazioni sugli utenti (mediante pagine di registrazione, pagamenti online, informazioni rilasciate dai browser, ecc..) e spesso queste vengono fornite a terze parti **all'insaputa** dell'utente, non fornendo a quest'ultimo la possibilità di avere un controllo sul loro uso, anche quando a conoscenza del fatto che i dati vengono raccolti. È facile intuire come queste operazioni possono portare alla **violazione della privatezza** dei dati. Vediamo alcuni esempi.

1. LINK REFERENZIALI

Quando si clicca su un link che porta ad un altro sito web, quest'ultimo, mediante il campo **referer** dell'header HTTP, viene a conoscenza del sito web di partenza.

Questo sistema può essere usato per scopi leciti, come ad esempio tracciare il comportamento dell'utente all'interno del sito, ma può rivelare informazioni sensibili nel caso in cui l'**URL** di partenza contenga informazioni personali. Esempio:

http://www.sito.com/order?name=Alice&address=via+milano+18&phone=34799999999

Se tale URL viene riportato tramite il **referer link** al prossimo sito web, l'amministratore di quest'ultimo viene a conoscenza di dati sensibili (nome, indirizzo e numero telefonico) senza che l'utente possa avere modo di negarlo.

2. ANONYMIZER

Per mantenere l'anonimato, alcuni utenti utilizzano degli **anonymizer** che agiscono come proxy (sdoppiano la comunicazione tra client e server e fanno da intermediari) ma **non si ha un vero anonimato** in quanto i gestori di tali proxy hanno accesso alle informazioni e gli utenti **devono fidarsi** che questi non li trasferiscano a terze parti.

3. COOKIE

I cookie sono stringhe di testo di piccola dimensione inviate dal server al client (di solito un browser) e poi rimandati indietro dal client al server ogni volta che il client accede allo stesso sito. I cookie possono essere **temporanei** se rimangono memorizzati finché non si esce dal browser, **persistenti** se rimangono memorizzati finché non si eliminano o non scadono, **third party cookie** se associati ad immagini di un sito con nome dominio diverso da quello attualmente visitato.

I cookie non sono mica dannosi ma dannoso può essere l'utilizzo improprio che se ne fa, ad esempio quando possono essere letti da siti diversi. È il caso di aziende che fanno advertising network come la DoubleClick.

4. WEB BUG

Detti anche **web beacon** sono immagini invisibili (trasparenti o di dimensione ridottissima, come 1x1) che vengono inseriti maliziosamente nella pagine web col fine di **monitorare il comportamento degli utenti**. Com'è possibile registrare informazioni con un'immagine? Semplicemente si registrano in file di log tutte le informazioni inviate dal browser mediante l'header HTTP (indirizzo IP, referer, orario, tipo di browser, ecc..) quando questo fa richiesta di caricamento dell'immagine. Queste informazioni possono essere utilizzate da aziende di marketing.

5. SPYWARE

Sono altri software il cui scopo è quello di raccogliere informazioni sugli utenti **all'insaputa di questi**. Essendo che non modifica alcun dato, non è ritenuto illegale, per lo meno negli USA.

6. NUOVE TECNOLOGIE

Attualmente vi sono nuove tecnolgie che se da un lato permettono lo sviluppo di applicazioni di pubblica utilità, dall'altro possono portare a violazioni della privacy degli utenti. Alcuni esempi sono:

- L'**ubiquitous computing**: permette ai device degli utenti di comunicare con l'infrastruttura che li circonda (per esempio per fornire assistenza agli anziani). Può portare a violazioni di privacy in quanto il movimento degli utenti, ovvero ciò che fanno, dove si trovano, ecc... viene continuamente monitorato.

- Il **global position system** (**GPS**): anche questa può essere usata per tracciare le persone.

In una società globalizzata, il diritto all'informazione e alla privatezza devono essere **legalmente disciplinati** non solo a livello nazionale ma anche internazionale. L'**Unione Europea** ha così predisposto un sistema normativo e giurisdizionale in materia di tutela della privatezza che ha incentivato molti Stati membri ad introdurre nuovi istituti.

L'**articolo 8** della **Carta dei diritti fondamentali dell'UE di Nizza** rappresenta l'evoluzione della tutela della privacy a livello internazionale, riconoscendo il diritto di protezione dei dati personali, la lealtà del trattamento, il consenso dell'interessato, l'accessibilità della persona interessata ai propri dati, ribadendo che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Direttiva 95/46: tutela le persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione dei dati.

Direttiva 97/66: trattamento dei dati personali e tutela della vita privata nel settore delle telecomunicazioni.

Queste due direttive introducono il concetto di **consenso dell'interessato** e la **facoltà** di decidere di non comparire sull'elenco telefonico e di mantenere l'anonimità nelle chiamate.

Direttiva 2002/58: trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche.

Quest'ultima direttiva garantisce la libertà di circolazione dei dati personali all'interno della CE e vieta qualsiasi forma di intercettazione delle comunicazioni e dei relativi dati, salvo espresso consenso degli interessati o autorizzazione legale.

Gli Stati membri devono garantire un trattamento leale e lecito dei dati che comunichi preventivamente le finalità della rilevazione e del trattamento, l'esattezza, l'aggiornamento e la conservazione per un periodo non superiore a quello strettamente necessario per il raggiungimento dello scopo.