

Cookie: cosa sono, come vengono usati e quando sono pericolosi.

I cookie sono uno degli argomenti più discussi di Internet concernenti il diritto alla privacy, questo perché spesso gli utenti si chiedono come fanno i siti Internet a ricordare la loro identità dopo il primo accesso, oppure come fanno i negozi online a conservare gli oggetti che abbiamo inserito nel carrello? La risposta sta nei cookie.

In informatica i **cookie HTTP** (più comunemente denominati **Web cookie**, **tracking cookie** o semplicemente **cookie**) sono righe di testo usate per eseguire autenticazioni automatiche, tracciatura di sessioni e memorizzazione di informazioni specifiche riguardanti gli utenti che accedono al server, come ad esempio siti web preferiti. Nel dettaglio, sono stringhe di testo di piccola dimensione (arrivano a 4 KB), in formato *txt* o *xml*, inviate da un server ad un Web client (di solito un browser) e poi rimandati indietro dal client al server (senza subire modifiche) ogni volta che il client accede alla stessa porzione dello stesso dominio web. Sono informazioni immesse sul tuo browser quando visiti un sito web o utilizzi un social network con il tuo pc, smartphone o tablet. Ogni cookie (in inglese, "biscotto") contiene diversi dati come, ad esempio, il nome del server da cui proviene, un identificatore numerico, ecc..

Questi cookie, cosiddetti **tecnici**, sono spesso utili, perché possono rendere più veloce e rapida la navigazione e fruizione del web, perché ad esempio intervengono a facilitare alcune procedure quando fai acquisti online, quando ti autentichi ad aree ad accesso riservato o quando un sito web riconosce in automatico la lingua che utilizzi di solito. Una particolare tipologia di cookie, detti **analytics**, sono poi utilizzati dai gestori dei siti web per raccogliere informazioni, in forma aggregata, sul numero degli utenti e su come questi visitano il sito stesso, e quindi elaborare statistiche generali sul servizio e sul suo utilizzo. Altri cookie, di **proliferazione**, possono invece essere utilizzati per monitorare e profilare gli utenti durante la navigazione, studiare i loro movimenti e abitudini di consultazione del web o di consumo (cosa comprano, cosa leggono, ecc.), anche allo scopo di inviare pubblicità di servizi mirati e personalizzati (c.d. Behavioural Advertising).

Dunque, ogni volta che ci colleghiamo con un sito Internet, il browser preleva automaticamente tutti gli elementi che compongono le pagine visualizzate e li salva in una cartella temporanea denominata **cache**, ma memorizza sul disco fisso anche i cookie, che **non rappresentano di per sé un pericolo**, anzi, il loro impiego è di fondamentale importanza, per il corretto funzionamento dei negozi online, per conservare il login in un blog, in un'area privata, in un forum, od in una qualunque applicazione web che richieda qualsiasi forma di autenticazione.

I siti hanno iniziato ad usare questo tipo di cookie nella seconda metà degli anni '90, e da allora i cookie hanno conosciuto una massiccia diffusione. Ad oggi, la stragrande maggioranza dei siti lascia cookie nel tuo computer (ad esempio, il 92% dei siti in UK lascia cookies). Tutti – ma assolutamente tutti – i siti più popolari al mondo (inclusi Google, Yahoo!, Facebook, Wikipedia, Microsoft etc) lasciano cookie. Ogni singola pagina che visiti lascia numerosi cookie.

La gestione di cookie è completamente dipendente dal browser web che si è deciso di impiegare: il programma che si utilizza per "navigare" in Rete può **accettare i cookie, rifiutarli o limitarne l'uso solo a determinati siti**. Il contenuto dei cookie può essere poi ovviamente eliminato ogniqualvolta lo si dovesse ritenere opportuno. Per procedere, è necessario accedere alla finestra delle impostazioni del browser ed utilizzare l'apposita funzionalità di **rimozione dei cookie**. Tale strumento è di solito inserito nella medesima schermata attraverso la quale è possibile eliminare la *cache*. Se un cookie è stato creato da un sito al quale si accede frequentemente e che prevede il controllo delle informazioni personali dell'utente, questo può contenere una password o un codice per la verifica dell'identità dell'utente stesso in forma cifrata. Tali cookie non dovrebbero essere

eliminati per evitare di dover reintrodurre ogni volta manualmente tutte le informazioni in esse conservate. **I cookie non possono trasportare virus o malware**, né possono trasferire elementi dannosi ad altri utenti quindi non vanno temuti o cancellati in continuazione. Il problema principale dei cookies è legato alla **privacy dell'utente**. Tramite i cookie è possibile, per un sito dannoso che vuole rubare informazioni su internet, conoscere la cronologia dei siti visitati da una persona su quel computer e sfruttare tali informazioni per inviargli pubblicità mirata ai suoi interessi.

Ci sono quindi due modi per difendersi dai cookie traccianti. Si può navigare senza caricare i cookie, simulando quindi una sessione di visite ai siti internet come fosse sempre la prima volta. Questo modo di navigare è la cosiddetta funzione di navigazione in incognito o privata dei browser che può essere attivata su Chrome, Opera, Internet Explorer o Firefox.

Se invece si volessero bloccare a monte tutti i cookie traccianti allora si possono usare alcune estensioni per non farsi tracciare online dai siti bloccando la raccolta di dati personali. Fondamentalmente vengono consentiti solo alcuni cookies, bloccando quelli provenienti da siti pericolosi come le agenzie di pubblicità più intrusive. Su Internet Explorer è possibile cancellare i cookie scaduti per rendere il browser più sicuro. In generale si può invece leggere la guida per eliminare i cookie da Firefox, Chrome e Internet Explorer.

I cookie e la privacy

Considerata la particolare invasività che i *cookie di profilazione* possono avere nell'ambito della sfera privata degli utenti, la normativa europea e italiana prevedono che l'utente debba essere adeguatamente informato sull'uso degli stessi ed esprimere il proprio valido consenso all'inserimento dei cookie sul suo terminale.

In particolare, con il provvedimento "**Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie**" dell'8 maggio 2014 [doc web n. 3118884] il Garante per la protezione dei dati personali ha stabilito che quando si accede alla home page o ad un'altra pagina di un sito web che usa cookie per finalità di profilazione e marketing deve immediatamente comparire un banner ben visibile, in cui sia indicato chiaramente:

- 1) che il sito utilizza cookie di profilazione per inviare messaggi pubblicitari mirati
- 2) che il sito consente anche l'invio di cookie di "terze parti"
- 3) un link a una informativa più ampia, con le indicazioni sull'uso dei cookie inviati dal sito, dove è possibile negare il consenso alla loro installazione direttamente o collegandosi ai vari siti nel caso dei cookie di "terze parti"
- 4) l'indicazione che proseguendo nella navigazione (ad es., accedendo ad un'altra area del sito o selezionando un'immagine o un link) si presta il consenso all'uso dei cookie.

Utilizzo cookie sul sito:

- Questo sito non utilizza i cookie per inviare messaggi pubblicitari in linea con le preferenze dell'utente.
- Il sito non consente l'invio dei cookie di terze parti.

- Il sito utilizza solamente i cookie in maniera anonima per censire il traffico sul sito.
- Continuando con la navigazione si accettano implicitamente i cookie che il sistema andrà ad installare.