I COOKIE

non accettare caramelle dagli sconosciuti

Graziano de' Petris[*]

[*] *Responsabile dell'Ufficio privacy e trattamento dei dati sensibili dell'Azienda Ospedaliero – Universitaria "Ospedali Riuniti" di Trieste, Vicepresidente APIHM*

Cosa sono i Cookie

I cookie sono stringhe di testo (o dati senza significato apparente) che un *server web* invia al *browser* del PC mentre si visita un determinato sito e che vengono salvati in un'apposita cartella sul disco locale. Nei sistemi Windows, ad esempio, la cartella è denominata "Temporary Internet Files" .

I cookie immagazzinano nel PC alcune informazioni sulla navigazione dell'utente, esistono da quando esiste il Web e sono stati inventati per facilitare la navigazione: ogni volta che si visita un sito, il PC (o lo Smartphone, oppure il Tablet) salva al suo interno informazioni che poi, al prossimo collegamento, rinvia al *server web* che ospita quel sito, affinché questo ricordi chi siamo e possa così creare una "*esperienza di navigazione"* personalizzata per noi.

Esistono due tipi di cookie: i *coockie temporanei* e i *cookie permanenti*. I cookie temporanei (o coockie di sessione) vengono memorizzati durante ogni sessione di collegamento e vengono rimossi dal dispositivo alla chiusura del browser. I cookie permanenti o (coockie salvati in locale) rimangono archiviati nel nostro dispositivo e vengono cancellati solo quando raggiungono una "data di scadenza" prefissata o quando vengono *rimossi manualmente* dall'utente. Questo tipo di cookie vengono in genere usati dai siti per ottimizzare la navigazione, ad esempio ricordando le credenziali di accesso ad un sito oppure memorizzando gli oggetti del carrello degli acquisti, per agevolare l'utente e farlo sentire più a suo agio mentre naviga in quel tal sito. I coockie permettono infatti, ad esempio, di farci ritrovare la medesima configurazione personalizzata che avevamo impostato nella casella della mail web o di ricevere informazioni meteorologiche in tempo reale in base al nostro CAP di residenza, anche se non abbiamo un sistema di localizzazione attivo. Tra i cookie permanenti, però, vi possono anche essere cookie di aziende terze rispetto al sito che si sta visitando, che vengono inseriti a seguito di accordi commerciali tra i gestori del sito e altre società (i "terzi", appunto). Questi cookie possono anche tracciare l'intera nostra attività online allo scopo di *profilare il consumatore*; essi vengono usati spesso da agenzie pubblicitarie internazionali, allo scopo di conoscere i siti e le pubblicità che visualizziamo maggiormente e trarne vantaggio economico, ad esempio attraverso la vendita di elenchi di indirizzi mail di potenziali consumatori, classificati per età, sesso, area geografica, professione, reddito, interessi e altre informazioni, anche sensibili. Attraverso cookie di questo tipo si possono ottenere informazioni sufficienti per creare in brevissimo tempo un profilo completo sulle nostre preferenze o addirittura un intero dossier su di noi.

I cookie sono un pericolo per la nostra privacy?

Se permettiamo ai cookie di avere accesso ai nostri PC, Smartphone o Tablet, la navigazione sarà certamente più veloce e comoda, ma fino a che punto le nostre informazioni personali saranno al sicuro?

In rete si trovano da tempo molte discussioni sul binomio “cookie e privacy”; generalmente si tende a ritenere che non siano pericolosi, nell’ottica di un bilanciamento tra quante informazioni siamo disposti a concedere su di noi e quanti benefici possiamo ottenere in cambio. Ciò può essere vero, ma a patto di adottare alcuni accorgimenti.

E’ fondamentale prestare sempre molta attenzione, perché attraverso i cookie si possono, ad esempio, raccogliere informazioni di carattere estremamente personale o perfino scatenare veri e propri attacchi informatici (definiti *the man in the browser*). In letteratura sono già state dimostrate più volte alcune vulnerabilità dei vari browser, che permettono anche di accedere ai dati personali contenuti in altre cartelle del PC. I produttori dei browser sono però sempre molto veloci nel correre ai ripari con opportuni aggiornamenti di sicurezza ogni volta che una vulnerabilità viene segnalata. Dopotutto è nel loro interesse che gli utenti considerino quel tal browser sicuro e continuino ad utilizzarlo. Questa tipologia di attacchi è quindi poco diffusa e, per un utente normale, poco pericolosa.

Con i cookie, però, si possono raccogliere anche informazioni molto personali a scopo commerciale o a scopo di controllo comportamentale. Tutto questo, ovviamente, da sempre. Siccome però negli ultimi tempi è molto aumentata la sensibilità dell’opinione pubblica sul tema, sempre più gestori di siti web stanno iniziando a prendere in considerazione la protezione delle informazioni personali dei propri utenti, ad esempio bloccando i cookie permanenti di aziende terze (non certo però di quelle con le quali sono in partnership commerciale, ovviamente).

I cookie e il Garante per la protezione dei dati personali

L’Autorità Garante della privacy, resasi conto della sempre maggiore intrusione operata dai cookie nella sfera strettamente personale degli individui e dei potenziali pericoli conseguenti, è intervenuta con il Provvedimento dell’8 maggio 2014, che dava tempo fino all’8 giugno 2015 ai gestori dei siti web per segnalare nell’informativa privacy (obbligatoria in ogni sito web) come vengono gestite le informazioni personali degli utenti e come vengono utilizzati i cookie. Nel provvedimento vengono identificate tre diverse tipologie di cookie, e vengono prescritte altrettante azioni che i gestori debbono, di conseguenza, attuare: per la prima tipologia di cookie, cioè se vengono utilizzati soltanto cookie tecnici (atti esclusivamente a monitorare tecnicamente il buon funzionamento del sito), anche se questi sono di di terze parti (come a titolo di esempio, i collegamenti a Tweeter o a Facebook spesso presenti in molti siti), ma il sito impedisce alla parte terza di ricevere informazioni sull’identità degli utenti che si collegano, è sufficiente indicarlo chiaramente nell’informativa; se invece i cookie sono della seconda tipologia, se cioè vengono utilizzati anche per profilare la navigazione degli utenti (cookie di profilazione), ciò deve essere indicato da un *banner* che deve comparire non appena ci si collega al sito e l’indicazione deve essere accettata esplicitamente dall’utente, che deve quindi cliccare su “ok” o “accetto” dopo aver letto l’indicazione, allo scopo esprimere la sua chiara volontà di proseguire; se, infine, i cookie sono della terza tipologia, se cioè vengono utilizzati anche da terze parti per la profilazione delle abitudini degli utenti, oltre all’obbligo di indicarlo con un banner, vige l’obbligo di dover notificare il fatto al Garante e ciò anche se la società che gestisce il sito ha sede all’estero. In quest’ultimo caso il trattamento dei dati viene inserito in un apposito registro dei trattamenti di dati personali, pubblicamente consultabile, e il gestore del sito si impegna ad utilizzare tutti i dati raccolti nel rispetto delle normative privacy vigenti in Italia.

Cosa possiamo fare in pratica per proteggerci

La prima cosa da sapere è che non può esistere una norma o una legge che protegga dall'imbecillità o dall'ignoranza. I migliori difensori della nostra privacy siamo sempre e soltanto noi stessi. Se desideriamo diffondere la minor quantità possibile di informazioni su di noi, bisognerà fare in modo che i cookie non registrino le nostre abitudini di navigazione, rimuovendoli o impedendo che vengano registrati.

Cancellare i cookie al termine di ogni sessione di collegamento

La cronologia di navigazione e i cookie possono essere cancellati in qualsiasi momento. Questa impostazione è presente nel menù di configurazione di tutti i browser.

Cambiare le impostazioni del browser

Nel caso in cui si desideri fornire soltanto alcune indicazioni, quasi tutti i browser offrono la possibilità di decidere quali informazioni vengono tracciate dai cookie. Per farlo è sufficiente controllare le *impostazioni sulla privacy* nel menù del browser che si sta utilizzando ed eventualmente modificarle.

Utilizzare i componenti aggiuntivi

Quasi tutti i browser hanno la possibilità di scaricare alcuni *componenti aggiuntivi*; alcuni di questi aiutano a gestire i cookie in modalità avanzata. Con i componenti aggiuntivi si può, ad esempio, decidere quali informazioni possono essere tracciate e per quanto tempo e quali invece per niente.

Condividere le informazioni personali moderatamente

Quando si usa un *computer pubblico* (cioè non un dispositivo personale), bisogna seguire alcune regole di buon senso. Per principio non andrebbero mai digitate informazioni di carattere personale, che potrebbero essere salvate dai cookie, e bisogna assicurarsi sempre e comunque di effettuare il log-out quando si abbandona la sessione.