Revista Universul Juridic ● nr. 2, februarie 2015, p. 13-15

CUM SPORIM CONFIDENȚIALITATEA NAVIGĂRII ONLINE

Andreea LISIEVICI

ABSTRACT

How to increase online navigation confidentiality

The author presents some methods that facilitate the insurance of an internet traffic without data being collected by various online services, in the current judicial context.

The article contains recommendations on the browser's setting, the settings with regard to behavioural advertising and dedicated applications for the browser.

In closing, the author mentions a series of extensions that contribute to an increase in confidentiality and recommends some necessary reading material for achieving this purpose.

Keywords: *confidentiality; online navigation; browser; settings; behavioural advertising; applications; extensions; necessary reading.*

Navigarea pe Internet presupune colectarea unor date de către deținătorii site-urilor vizitate, fie că acestea sunt magazine online, platforme de social media, servicii de email sau altele. Totuşi, de cele mai multe ori datele colectate nu sunt limitate la cele necesare accesării paginilor vizitate, iar utilizatorii de Internet devin din ce în ce mai conştienți de acest lucru. De altfel,*studiul efectuat de Microsoft la sfârşitul lunii decembrie 2014* în 12 țări (SUA, Franța, Germania, Japonia, Coreea de Sud, Brazilia, India, Rusia, China, Turcia, Africa de Sud şi Indonezia) relevă faptul că un procent semnificativ din utilizatori declară că nu sunt complet informați cu privire la informațiile care sunt colectate despre ei. Nu în toate cazurile vorbim de o lipsă de informare din partea site-urilor în cauză, însă de foarte multe ori această informare se ascunde în cadrul unor „Termeni şi condiții" stufoase, pe care larga majoritate a utilizatorilor bifează că le acceptă fără să citească până la capăt (sau chiar deloc).

În materie de regim juridic, în România ca şi în Uniunea Europeană în general, stocarea de cookies pe terminalele utilizatorilor este condiționată de acordul expres (art. 4 alin. 5 din Legea nr. 506/2004). Însă faptul că un site solicită acest acord nu înseamnă şi că oferă informații complete, corecte şi mai ales uşor de înțeles cu privire la datele care se colectează, durata şi scopul prelucrării acestora. Un site poate folosi *cookies* pentru a stoca preferințele utilizatorului (de exemplu, reținerea identității la logarea ulterioară), pentru a-şi analiza traficul, pentru a implementa platforme de comentarii ori soluții de plată, etc., iar toate acestea sunt justificate şi

perfect acceptabile. Dar nu acelaşi lucru se poate spune despre cookie-urile care analizează istoricul de navigare pe o perioadă de multe ori foarte lungă pentru a furniza publicitate comportamentală (adică particularizată tocmai în funcție de acel istoric), sau de cele asociate plugin-urilor rețelelor de socializare implementate pe site-uri terțe, prin care vizitatorii pot selecta un buton pentru a aprecia sau distribui o anumită informație/pagină (Like, Share, Tweet, +1) însă care colectează date despre utilizatorii logați în rețelele respective de socializare, chiar dacă butoanele nu sunt folosite.

Colectarea datelor referitoare la navigarea pe internet nu are, de cele mai multe ori, un scop ilegal sau imoral. Însă pe lângă riscul ca aceste informații să fie furate, compromise ori divulgate, riscul major este ca aceste informații să fie folosite, poate chiar de cei care le-au colectat, împotriva utilizatorului – de exemplu, *prețul unui produs să fie mai mare în funcție de istoricul de navigare*. Tocmai de aceea, în materia asigurării securității şi confidențialității navigării pe internet, primul şi totodată cel mai eficient responsabil este chiar utilizatorul în sine. Având în vedere acest lucru, am pus laolaltă mai jos **câteva mijloace care facilitează asigurarea unui trafic pe internet fără urme colectate de diverse servicii online**. Trebuie menționat că unele din acestea (în special add-on-urile pentru browser) pot conduce la o navigare mai anevoioasă, de exemplu prin necesitatea logării mai dese.

I. Setările browserului

Browserele, dispozitive mobile şi aplicațiile sunt de multe ori setate implicit pentru a partaja datele personale. Ca urmare, fiecare utilizator trebuie să verifice şi, la nevoie, să modifice aceste setări – există resurse online pentru a învăța cum să *ajustați setările de privacy în toate marile browsere*, ori pe terminalele mobile.

II. Setările privind publicitatea comportamentală

Dacă vreți să nu primiți publicitate comportamentală, atunci puteți administra această opțiune pentru mai multe platforme o dată, pe portalul dedicat *http://www.youronlinechoices.com/ro/optiunile-mele*. Desigur, asta nu înseamnă dispariția publicității, oricât de supărătoare ar fi ea, ci doar că reclamele plasate de site-urile indicate (în prezent 96 societăți) nu vor ține cont de istoricul de navigare şi, implicit, şi că acest istoric nu va fi monitorizat. Alte cookie-uri nu vor fi afectate.

III. Aplicații dedicate pentru browser

În materie de browsere, Firefox stă foarte bine la capitolul privacy, având atât opțiunea de a comunica site-urilor să nu monitorizeze traficul, cât şi o modalitate de stocare locală criptată a parolelor. În plus, i se pot adăuga o sumedenie de extensii care să sporească confidențialitatea navigării.

De exemplu, *Ghostery* este o extensie care blochează o sumedenie de cookie-uri, widget-uri şi beacon-uri folosite de diverse servicii. Are o interfață prietenoasă şi afişează pe fiecare site accesat ce mijloace de tracking a găsit şi dacă

sunt blocate sau nu. Funcționează atât cu reguli permanente, cât şi cu opțiuni temporare selectate de la caz la caz.

De asemenea, *Better Privacy* este o extensie specifică Firefox şi care şterge un tip special de cookie-uri numite *LSO (local shared objects) sau Flash cookies*. Spre deosebire de cookie-urile normale, LSO nu sunt stocate în browser şi deci nu pot fi administrate de acesta şi nici blocate de Ghostery.

Nu în ultimul rând, *Blur* (până recent DoNotTrackMe) este un serviciu foarte complex, care oferă adrese de email mascat cu autoforward la o adresă master (Masked Emails), blocarea trackerelor (asemănător cu Ghostery), administrarea parolelor şi un serviciu de portofel electronic a cărui componentă principală, Masked Cards (creează un număr de card nereal care se trimite comerciantului), nu este disponibilă decât în SUA. Blur este foarte util dacă nu vreți ca toate site-urile pe care vă creați cont să dețină adresa reală de email, în schimb doriți să puteți citi toate mesajele de pe o singură adresă, şi este şi foarte uşor de folosit. Ca efect secundar, în cazul spam-urilor primite pe o adresă mascată, se poate vedea exact pentru ce site ați creat-o şi, deci, ce site nu asigură confidențialitatea datelor.

Alte extensii care contribuie la sporirea confidențialității includ *HTTPS Everywhere*, *AdBlock Plus*,*Beef Taco (Targeted Advertising Cookie Opt Out)* – doar pentru Firefox, şi toată *colecția de add-on-uri privacy* pentru Firefox facută de Mozilla.

În plus față de cele de mai sus, *Ghidul de confidențialitate* ApTI şi infograficul *9 Tips for Keeping Your Internet Usage Private* sunt cu siguranță lecturi necesare.

Spor la navigare privată!