



Evitarea profilării la navigarea pe Internet

Drd. Marius NEBANCEA

Prof.univ.dr. Ciprian RĂCUCIU

RELEVANȚA TOPICULUI

- 5.6 miliarde de utilizatori de internet
- 15.87 TB de date create zilnic
- >5000 de firimituri digitale/user zilnic
- 1.7 MB/s date per user mediu de internet, zilnic,- 147 GB/zi

<https://datareportal.com/global-digital-overview>
<https://edgedelta.com/>
<https://soax.com/>
<https://www.statista.com/>
<https://datareportal.com/>

FIRIMITURILE DIGITALE – Digital breadcrumbs

Firimituri digitale – fragmente de informații pe care le lăsăm în urmă ca urmare a folosirii internetului sau a dispozitive digitale

Firimituri active – date lăsate intenționat

- ☐ Căutări în motoare de căutare
- ☐ Postări, comentarii, recenzii
- ☐ Formulare de date
- ☐ Achiziții online
- ☐ Mesaje trimise, etc.

Firimituri pasive – informații colectate fără acțiune directă

- ☐ Istoric de navigare
- ☐ Adrese IP
- ☐ Informații despre dispozitive
- ☐ Locație și telemetrie
- ☐ Metadata, etc.

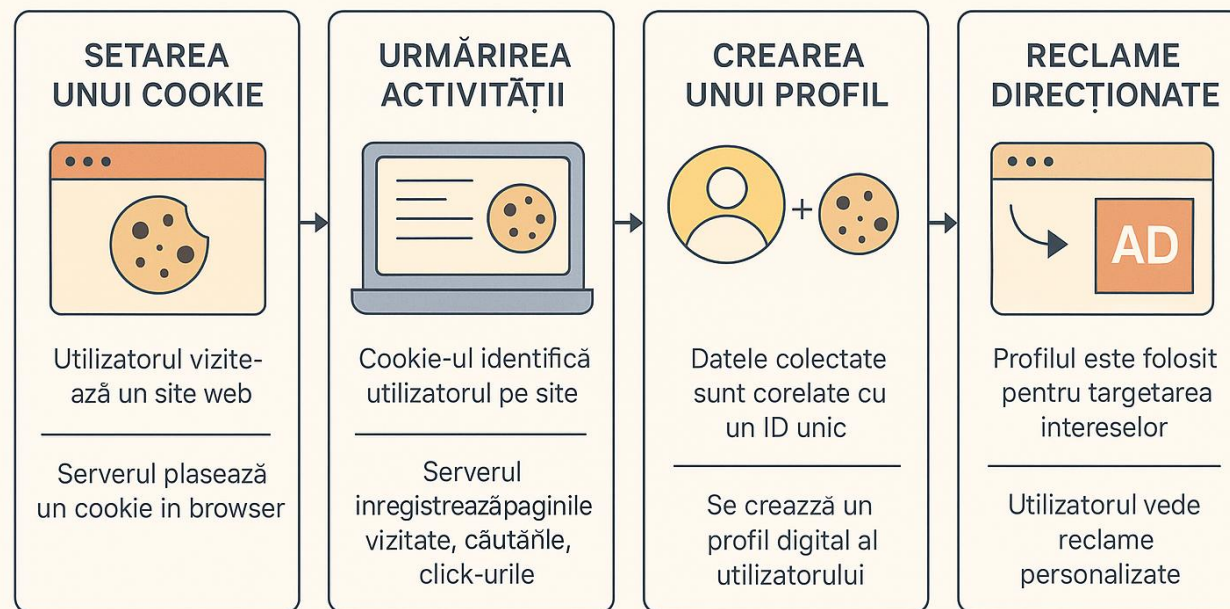
Profilarea prin cookies

Evitare a profilării :

- blocarea instalării de cookie third-party în browsere
- folosirea unor extensii de blocare (uBlock, Adblock Plus, etc)
- ștergerea periodică a cookie-urilor din browser
- folosirea browser-ului în mod Incognito pentru a nu salva cookie
- acceptarea doar a cookie-urilor esențiale

PROFILAREA PRIN COOKIE-URI

Procesul de colectare și analiza a datelor despre activitatea utilizatorului pe un site web, folosind cookie-uri.



Profilarea prin Fingerprinting

Evitare a profilării :

- folosirea unor browsere care protejează împotriva fingerprinting-ului:
 - Tor Browser (cel mai bun la acest capitol)
 - Firefox (cu protecție strictă activată)
 - Brave (are anti-fingerprinting încorporat)
- evitarea extensiilor inutile, care pot face mai ușoară identificarea.
- dezactivarea JavaScript, dar asta va afecta funcționarea multor site-uri.
- folosirea unor extensii dedicate:
 - CanvasBlocker (Firefox)
 - Trace
 - Privacy Badger (ajută parțial)
- uniformizarea comportamentului digital – o configurație „standard” este mai greu de identificat.

BROWSER FINGERPRINTING

Ce este și cum se face?



Ce este:
metodă de colectare
a datelor fără
utilizarea contului
utilizatorului



Cum funcționează:
colectează datele
tehnice ale
browserului și
sistemului utilizat



Se crează o bază de
date care permite
monitorizarea în
timp și geografic a
utilizatorului

Profilarea prin scripturi și pixeli

Evitarea profilării:

- blocarea scripturilor și a pixelilor cu extensii:
 - uBlock Origin
 - Privacy Badger
 - NoScript (pentru utilizatori avansați)
- folosirea unui browser cu protecție anti-tracking:
 - Brave, Firefox (cu Enhanced Tracking Protection), Tor
- dezactivarea JavaScript (unele site-uri nu vor funcționa corect)
- folosirea unui client de e-mail care blochează pixelii din emailuri, cum ar fi ProtonMail sau Thunderbird.
- scanarea site-urile vizitate cu instrumente specializate:

PROFILARE PRIN SCRIPTURI SI PIXELI INVIZIBILI



CE ESTE



CUM FUNCȚIONEAZĂ

Scripturile colectează discret date în timpul navigării, în timp ce pixelii ascunși trimit informațiile către serverele terților.



COLECTARE DE DATE

Aceste tehnici pot înregistra vizitele paginilor, clicurile, timpul petrecut și alte interacțiuni ale utilizatorului pe site.

Profilarea tracking cross-site și rețele publicitare

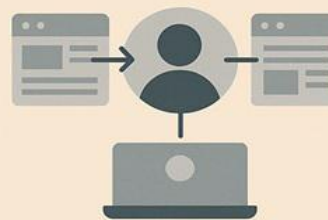
Evitarea profilării:

- blocarea cookie-urile terțe în browser
- folosirea unor extensii anti-tracking:
 - uBlock Origin
 - Privacy Badger
 - Ghostery
- atenție la bannerele de tip „Accept cookies”.
- nu se vor utiliza conturi personale pe site-uri unde nu este nevoie
- evitarea logării cu conturi Google/Facebook
- folosirea unui browser cu protecție anti-tracking: Brave, Firefox (cu ETP), Tor.

PROFILAREA PRIN TRACKING CROSS-SITE ȘI REȚELE PUBLICITARE

CE ESTE

Colectarea datelor despre utilizatori de la mai multe site-uri



CUM FUNCȚIONEAZĂ

Rețelele publicitare urmăresc comportamentul pe site-uri pentru a afișa reclame personalizate



Profilarea prin localizare și date de geolocalizare

Evitarea profilării:

- dezactivarea localizării permanente în aplicațiile care nu au nevoie reală de ea
- selectivitate cu permisiunile – fără acceptarea accesului la locație decât unde este strict necesar
- folosirea unui VPN – maschează IP-ul, deci și localizarea generală
- activează „location approximation” (acolo unde este disponibil) – oferă locație imprecisă în loc de cea reală
- utilizarea unor browsere care blochează cererile de geolocalizare automată (Firefox, Brave, Tor).

PROFILARE PRIN LOCALIZARE ȘI DATE DE GEOLOCALIZARE

CE ESTE ȘI CUM FUNCȚIONEAZĂ

CE ESTE

Colectarea și analiza poziției utilizatorilor folosind GPS-ul sau date despre rețele Wi-Fi și celulare.



CUM FUNCȚIONEAZĂ

Locația utilizatorilor este urmărită pentru a crea profiluri bazate pe locurile vizitate și pe rutină



Profilarea prin comportament și interacțiuni

Evitarea profilării:

- folosirea unor extensii care blochează analizatorii de comportament (ex: uBlock Origin, Privacy Badger)
- navigare în mod privat (Incognito) – reduce salvarea datelor comportamentale
- dezactivare JavaScript pentru site-urile care nu au nevoie de funcționalități complexe
- folosirea unui browser orientat pe confidențialitate, precum Brave sau Firefox cu Enhanced Tracking Protection

PROFILAREA PRIN INTERACȚIUNI ȘI COMPORTAMENT



CE ESTE

Profilarea prin interacțiuni și comportament implică monitorizarea acțiunilor și preferințelor utilizatorilor în timpul navigării pe internet.

CUM FUNCȚIONEAZĂ



1 Site-urile urmăresc interacțiunile precum clicuri, vizionari de conținut și pagini vizitate



2 Aceste date sunt utilizate pentru a analiza și înțelege comportamentele utilizatorilor



3 În baza acestei analize sunt create profile care permit personalizarea conținutului și recomandărilor

Profilarea prin conturi online și rețele sociale

Evitarea profilării:

- evitarea logării cu conturi mari (Google, Facebook) pe site-uri externe
- configurarea confidențialității conturilor (ex: cine poate vedea activitatea)
- folosirea aliasurilor și emailuri separate pentru diferite platforme
- fără inutile în profil (ex: școala, adresa, hobby-uri personale)
- utilizarea de extensii de browser care limitează trackerele rețelor sociale

PROFILAREA PRIN CONTURI ONLINE ȘI REȚELE SOCIALE

Înregistrarea unui cont



- nume, email, număr de telefon
- sex, vârstă, locație
- fotografie de profil

Completarea profilului și activitatea ta



- interese, hobby-uri
- paginile urmărite
- postări, like-uri, comentarii

Interacțiunile contribuie la „profilare algoritmică”



- like-uri la pisici → esti iubitor de animale
- urmărești brandu de lux → potențial client premium

Date din aplicații și site-uri externe



- conectare cu Google/Facebook pe alte-site-uri
- profil unificat: ce cumperi, ce citești, ce cauți



- supraveghere digitală extinsă
- manipulare comportamentală

Riscuri

Cum te poți proteja?

- supraveghere digitală extinsă
- manipulare comportamentală
- configurează confidențialitatea
- nu oferi date inutile în profil



RISCURILE PROFILĂRII

- pierderea intimității: activitatea ta online poate fi monitorizată fără consimțământ explicit.
- manipulare: conținutul personalizat poate fi folosit pentru a influența opinia publică
- discriminare: utilizatorii pot primi prețuri diferite sau pot fi excluși de la anumite oferte în funcție de profilul lor.
- vulnerabilități de securitate: datele colectate pot fi furate în urma unor breșe de securitate.
- supraveghere în masă: în unele state, aceste tehnici sunt folosite pentru control social.

Vă mulțumim!