675.46.32

| | |
|---|---|
| Nemzetközi Távközlési Adatvédelmi Munkacsoport | International Working Group on Data Protection in Telecommunications |

**Munkadokumentum. Webtracking és magánszféra: a kontextus, az átláthatóság és az ellenőrzés alapvető fontosságú marad***

53. Ülés, Prága, 2013. április 15-16.

**Bevezetés**

Ez a dokumentum az Internet-felhasználók alapvető jogain és szabadságain alapszik. Habár a dokumentum nem a különös technikai intézkedésekre koncentrál, abból indul ki, hogy a webtracking technikai eljárásainak jogszerűnek és megfelelőnek kell lenniük, működésüket e jogok szigorú keretei közé kell korlátozni. E keretek középpontja a választási lehetőségek és az ellenőrzés alapelvein nyugszik, mely elveket szabatosan az egyértelműség, az átláthatóság és a felelősség pillérjeire kell építeni. A webtracking alkalmazásának létjogosultsága nem magától értetődő, ezért az iparnak és egyéb nyomkövetést végző vállalkozásoknak folyamatosan olyan megoldásokat kell keresniük, amelyek e tevékenységet nem csupán az alapjogok és a privátszféra keretei közé szorítják, hanem összhangban vannak a „Privacy by Design" (megtervezett adatvédelem, vagyis a magánszféra védelmének figyelembe vétele már a technológia kifejlesztésekor) követelményével is.

2. Ebben a munkadokumentumban a Munkacsoport a webtracking és a magánszféra összefüggését tárgyalja. Jóllehet egyértelmű meghatározása nincsen, a webtracking [1] felfogásunk szerint nem más, mint az információs társadalom (a továbbiakban: Internet)[2] különféle szolgáltatásait igénybe vevő felhasználó aktivitására vonatkozó, egy számítógépről vagy más eszközről származó adatok gyűjtése, elemzése és alkalmazása abból a célból, hogy azokat változatos – jótékonysági, emberbaráti, kereskedelmi stb. – célok szerint csoportosítsák és elemezzék. Véleményünk szerint a webtracking ilyetén meghatározása a piackutatás különféle formáit is felöleli, például a kiterjedésmérést („outreach measurement" – az a kiterjedés, melyen belül az Interneten a felhasználók mindenhonnan hirdetéseket kapnak), a felhasználók viselkedésének mérését („engagement measurement" – vagyis hogy a felhasználó milyen mértékben lép interakcióba az internet-szolgáltatásokkal),

* A Munkacsoport „Working Paper on Web Tracking and Privacy: Respect for context, transparency and control remains essential 53rd meeting, 15-16 April 2013, Prague (Czech Republic) című dokumentumának fordítása (Dr. Könyves-Tóth Pál munkája) figyelemmel német nyelvű változatára is. Letölthető: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

[1] van Eijk (2012), The DNA of OBA: unique identifiers [egyértelmű azonosítók] [OBA = Online Behavioural Advertising = a felhasználó böngészési szokásaira épülő online reklám], URL: **http://www.campusdenhaag.nl/crk/publicaties/robvaneijk.html#definition-of-web-tracking**

[2] Megjegyezzük, hogy az IP-alapú technológia az információs társadalom sarkkövévé válik, és sok egyéb, korábban önálló technológiát integrál (konvergencia), amely felöleli a telefont (IP-telefónia), a televíziót (IPTV), a digitális újságok olvasását és bármely egyéb, digitális technológiára épülő médiát (ide értve az e-könyvet is). Az ezzel járó, magánszférát fenyegető kockázatok részletes elemzését lásd: Working Paper on Privacy Issues in the Distribution of Digital Media Content and Digital Television (Berlin, 2007); URL: **http://www.datenschutz-berlin.de/attachments/349/digit_en.pdf**

és az elért felhasználók számbavétele („audience measurement" – vagyis hogy az internetszolgáltatásokat interaktív módon felhasználók mikroprofiljai milyen mértékben képezhetők).[3]

3. Ez a dokumentum mindazokhoz az internet-szolgáltatókhoz, valamint szoftverfejlesztőkhöz és szolgáltatásnyújtókhoz szól, akik nyomkövetési technológiákat kínálnak vagy használnak. Tárgyalja a nyomkövetési technológiák fejlődését, és ezeknek a polgárok magánszférájára gyakorolt lehetséges hatásait. Azokkal a digitális nyomokkal foglalkozik, melyeket magunk mögött hagyunk, amikor az információs társadalom különféle szolgáltatásait egy internet-böngészővel igénybe vesszük, ide értve az egyedi azonosítókat /(„unique identifier"), amelyekhez a sütik nélkül működő technológiák segítségével jutnak hozzá.[4] Ide tartoznak továbbá más eszközök – pl. intelligens telefonok és intelligens TV-készülékek – böngészői is.

4. A dokumentum nem foglalkozik további specifikus kockázatokkal, amelyek a mobil eszközökön futó alkalmazásokból (appokból) származnak.[5] Mindazonáltal e dokumentum alapelveit egyéb szolgáltatások nyomkövető mechanizmusaira is alkalmazni kell.

5. E dokumentumban nem tárgyaljuk, hogyan lehet a védelmi mechanizmusokat (pl. a hozzájárulás jogszabályi követelményeit) megvalósítani. Megjegyezzük, hogy bár néhány jogrendszerben a webtracking – céljától függően – kifejezett hozzájárulást (opt-in) igényel, más jogrendszerekben a hozzájárulás megtagadásának (opt-out) lehetősége is elegendő a jogi követelmények teljesítéséhez, ha meghatározott feltételek teljesülnek. Egy sor egyéb korlátozásra is sor kerülhet, például különleges – pl. egészségi állapotra, politikai vagy világnézeti felfogásra vonatkozó – adatok feldolgozása, vagy gyermekek nyomkövetésének megakadályozása esetén.

**Háttér**

6. Az internet-használók aktivitásának megfigyelését szolgáló technikai lehetőségek az utóbbi tíz évben megsokszorozódtak, az „információs társadalom" több alapvető változást élt meg.[6] A webtracking nagyon szerény kezdeteit – amikor is egyes online szolgáltatást nyújtók felhasználóikat megfigyelve azt akarták megállapítani, hogy a felhasználók egy-egy weboldalt már korábban is felkerestek, s ott mit csináltak – az utóbbi időben a szolgáltatók szinte bizarr víziója követte. E vízióban a szolgáltató abba a helyzetbe kerül, hogy egy azonosítható felhasználó viselkedésének minden egyes vonatkozását a teljes Interneten megfigyelje. Ez egy adatalany teljes Internet használatának átfogó (szó szerint a bölcsőtől a sírig terjedő) történetévé válhat, és kiegészíthető a korábbi „offline világ" profiladataival (ideértve életünk minden lehetséges vonatkozását, melyről az adatügynökök információval rendelkeznek,

[3] JICWEBS Reporting Standards, URL: http://www.abc.org.uk/PageFiles/50/Web Traffic Audit Rules and Guidance Notes version2 March 2013 master.pdf

[4] Például passzív ujjlenyomat technikák, amelyek a HTTP
For example, passive fingerprinting techniques based on hashing the HTTP user agent and/or the IP address of the originating browser. Zum Beispiel die passive Fingerprinting-Technik, die auf dem Hashing des HTTP Endsystemteils bzw. der IP-Adresse des Ursprungs-Browsers basiert.

[5] Lásd pl.: 29. cikk szerinti adatvédelmi munkacsoport: 02/2013. vélemény az intelligens eszközökön használt alkalmazásokról, **http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_hu.pdf**

[6] A magánszféra Interneten való védelmével kapcsolatos irodalom áttekintése, amely a Magánszféra védelmének mérésével foglalkozó konferencia (Web Privacy Measurement, WPM) terméke, kimerítő összefoglalása a nyomkövetésre használt technológiáknak: **http://www.law.berkeley.edu/12633.htm**

többek között pénzügyeinkről, szabadidős tevékenységünkről, egészségi állapotunkról, politikai és vallási meggyőződésünkről, tartózkodási helyünkről).[7]

7. Ez a fejlődés – míg azt a szolgáltatók és a szélesebb üzleti világ más szereplői üdvözlik és támogatják, továbbá egyes politikusok is segítik nemzeti és regionális szinten – példátlan veszélyt jelent az információs társadalom valamennyi polgárának magánszférájára nézve. A legrosszabb esetben az általunk ismert világot egy globális panoptikummá változtathatja. Ennek offline ekvivalense: egy ismeretlen állandóan átnéz a vállunk fölött, függetlenül attól, éppen hol tartózkodunk (az utcán vagy látszólagos magánszféránkban, vagyis otthon), éppen mit csinálunk (tévét nézünk, online vásárolunk, újságot olvasunk vagy még intimebb aktivitást végzünk), s nincs tudomásunk arról, mikor néz ránk az ismeretlen és mikor nem.[8]

8. Egy ilyen fejlődés lehetséges következményei kézenfekvők, lehetséges súlyukat nem szabad alábecsülni, mert a magánszféra néhány lényeges alapelvét érvényteleníthetik vagy megsemmisíthetik, különösen az átláthatóságot és a polgárok ellenőrzési lehetőségét.[9] Még egyértelműbben: ez (a magánszféra védelmére nézve) a világ végét, legalábbis az általunk ismert világ végét jelentheti.

9. E vízió támogatói másrészről azt állítják, hogy ezek a kockázatok vagy egyáltalán nem léteznek, vagy hogy törekedtek arra, hogy ezekkel a veszélyekkel foglalkozzanak, és hatásukat legalább részben gyengítsék. A piaci érdekek képviselői erős ellenállást tanúsítanak annak elismerésével szemben, hogy az internet-használók egyedi azonosítói személyes adatnak minősülnek. Egy gyakran ismételt állítás: a felhasznált adatok többségét megfosztották azonosítóiktól (vagyis az adatokat anonimizálták), azokat többé meghatározott személyre nem lehet vonatkoztatni, ezért veszélyt sem jelentenek a polgárok magánszférájára nézve. Azt is gyakran állítják, hogy a viselkedési adatok csak a gépekhez kapcsolhatók, és így az esetek többségében egy meghatározott személyre egyáltalán nem vezethetők vissza.

10. Ezeknek az állításoknak azonban semmiféle tudományok igazolásuk nincsen, és figyelmen kívül hagyják azt a tényt, hogy a gépek – és különösen az intelligens telefonok – egyre inkább személyes eszközzé válnak, és könnyen lehetővé teszik az egyedi felhasználóhoz való kapcsolását. A nyomok növekvő mértékben különféle eszközökhöz köthetők. Tudományos bizonyíték is van arra, hogy sok látszólag anonim adat (pl. mobiltelefonok esetében a tartózkodási hely) az érintett felhasználóra visszavezethető (vagyis anonimizáltsága megszűnik), ha az adatbázis és az időkeret eléggé nagy. Újabb tudományos munkákban azt olvashatjuk, hogy teljességgel lehetetlen az „anonim" adatokat a visszaazonosítástól megóvni, ha egy adott viselkedés körülírására szolgáló időintervallum elég nagy (vagyis már koncepcionálisan is lehetetlen garantálni, hogy az „anonim" adatokat adott személyre ne lehessen visszavezetni). Ha ez igaz, áttörő fejlődésnek nézünk elébe, melynek révén egy sor kulcsfontosságú feltevés – mindenek előtt az, hogy a különféle típusú adatok felhasználása hogyan befolyásolja az egyén magánszféráját – értelmetlenné válik.[10]

---

[7] Az ügyfélkapcsolatok kezelésére szolgáló rendszerekben (Customer Relationship Management, CRM) használt szokásos fogalmak: Customer Lifetime [ügyfél-élettartam] és Customer Lifetime Value [ügyfél-tőkeérték].

[8] A helyzet azáltal még rosszabbodik is, hogy a panoptikum modern változata bármely adott egyén mozdulatát minden pillanatban rögzíti, függetlenül attól, hogy a teremőr éppen odanéz-e vagy nem.

[9] A nyomkövetés mint technológia nem transzparens: technikai szinten sok esetben a pixelek *[képpontok]* (pl. a web-beacon-ok [*kódfragmensek]*) és mini-web-oldalak (pl. iFrames) emberi szemmel nem láthatók.

[10] Vö.: Ohm, Paul: Broken Promises of Privacy: Responding to the Surprising *Failure of Anonymization (Megszegett adatvédelmi igéretek: felelet az anonimizálás meglepő hibájára)*, 2009. **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006**

11. Mindezen túl és kissé más beállításban, a mindennapok gyakorlati tapasztalata hozzájárul ahhoz, hogy az ipar által hangoztatott állításokat megkérdőjelezzük. Habár a hirdetések a technika szintjén egy gép címére irányulnak, végső soron nem a gép vásárolja meg a gyönyörű piros cipőt, hanem egy személy. Ezért az állítás, hogy a viselkedési adatok marketing célokra való feldolgozása „csupán" a gépekre korlátozódik, nagyon is olyan próbálkozásnak tekinthető, mely a probléma komolyságát tekintve víziónkat, mint a társadalom vízióját összezavarják, mivel a valóságban az ember és nem a gép az egyetlen példa, aki minden ilyen nyomkövetési műveletet „sikerre" képes vinni érintettjei számára (vagyis ha a piros cipőt végül megvásárolják).

**A nyomkövetési technológiák rövid története**

12. A fentebb körülírt fejlődés áttekintése szerény kezdetétől napjainkig a „cookie-technológia" közel 20 évvel ezelőtti, mérföldkőnek tekintett megjelenésével indítható: a HTTP-sütiket 1994-ben hozták divatba, elsősorban azért, hogy egy virtuális bevásárlókocsi megbízható használatával kapcsolatos „csekély" problémát megoldják. A Hypertext Transfer Protocol (HTTP) többnyire állapothiányos természete miatt, a végfelhasználói rendszerek akkoriban nem tudtak állapot információkat tárolni. Az állapot információk tárolása azonban felettébb fontos volt a virtuális bevásárlókocsik számára, hogy a kiválasztott árukat a vásárlás folyamán megjegyezzék. Az átláthatóság már ekkor is adatvédelmi kérdés volt, mert a sütik alkalmazásáról az átlagos vásárlót nem tájékoztatták. A sütiket ekkor általában a böngésző beállítás engedélyezte, de a sütik használatát a felhasználónak nem hozták tudomására.[11]

13. Az adatvédelmi és a biztonsági kockázatot jelent, hogy a süti-információk akaratlanul más weboldal-működtetőkhöz is eljutnak, aminek a mérséklése céljából az ún. „azonos eredet irányelv" (same-origin-policy) bevezetésére került sor. Ez a szabály azt jelenti, hogy sütiket csak ugyanarról a doménről lehetett olvasni, amely beültette azokat. Mindazonáltal fontos megjegyezni, hogy a World Wide Web Consortium (W3C) *[az Internetet illető technikák szabványait meghatározó testület]* egy új, a Cross Origin Resource Sharing (CORS) címet viselő szabványra tett javaslatot, amely az információcserét több specifikus domén között is megengedi. Ámbár a CORS [12] önkéntesen alkalmazható, ellentétes az „azonos eredet irányelvvel".

14. Csoportunk [13] már 1998-ban foglalkozott az Interneten megjelenő személyes adatok rendszeres gyűjtésével és felhasználásával kapcsolatos kérdésekkel. [14] Munkadokumentumában a P3P-vel (Platform for Privacy Preferences Project) *[platform az adatvédelmi információk cseréjére]*, a W3C által kifejlesztett protokollal foglalkozott, amely azt célozta, hogy harmadik fél sütijeit blokkolja, hacsak a felhasználó által felkeresett Internet-oldal fel nem ajánlott egy, a felhasználónak elfogadható P3P-policy-t.[15] Egyébként

[11] RFC 2109, HTTP State Management Mechanism, URL: **https://tools.ietf.org/html/rfc2109**. Jegyezzük meg, hogy a sütik tárolási technikáinak aktuális változatai többek között a Flash-Cookie-kat és az LSO-kat (Local Shared Objects) is felölelik, amelyeket a HTML5-ben megfelelő értékével figyelembe vesznek.

[12] Cross-Origin Resource Sharing, URL: **http://www.w3.org/TR/cors/** (felkeresve: 2013. május 30.)

[13] International Working Group on Data Protection in Telecommunications [IWGDPT, Nemzetközi Munkacsoport a Távközlési Adatok Védelmére.

[14] Common Position on Essentials for privacy-enhancing technologies (e.g. P3P) on the World Wide Web (Közös álláspont az adatvédelmet az Interneten erősítő technológiák (pl. P3P) alapvető jellemzőire vonatkozóan, Hong Kong, 1998. 04. 15.), URL: **http://www.datenschutz-berlin.de/attachments/178/priv_en.pdf**.

[15] A Platform for Privacy Preferences Project (P3P) lehetővé teszi, hogy az Internet-oldalak az adatvédelmi gyakorlatuk mindenkori módszereit szabványos formában kifejezzék, ami automatikusan lekérdezhető és a felhasználói ügynökök által egyszerűen értelmezhető. A P3P felhasználói ügynök lehetővé teszi, hogy a felhasználók tájékozódjanak az internet-oldal gyakorlatáról (mind géppel, mind ember által olvasható formában),

csupán egyetlen nagy böngészőkészítő alkalmazta a szabványt. Következésképpen a P3P-t az Interneten széles körben nem fogadták el.

15. A harmadik felektől származó sütik létfontosságúak a komplex digitális hirdetési ipar számára. A webtracking vállalkozások vezető marketing szakemberei 2008-ban a webanalitika és a webstatisztika jövőjéről tárgyaltak. Úgy képzelték, hogy öt év múlva a weboldal látogatás hagyományos statisztikája (a továbbiakban: First und Third Party Analytics) más webanalitikai szolgáltatásokat is integrál, mint például a videó szolgáltatásokat, widget-eket *[felhasználói felületek komponenseit]*, közösségi hálózatokat, játékokat, és keresőgépeket (a továbbiakban: webanalitikák).[16]

16. Manapság a webanalitikai adatok a gazdasági érték új formájaként jelennek meg. Habár ez a csoport nem kérdőjelezi meg azokat az előnyöket, amelyek a fogyasztói viselkedés mérése jelent a viselkedés alapú reklámozás (OBA) *[Online Behavioural Advertising]* (valós időben) számára, szilárd meggyőződése, hogy az efféle módszereket a magánszemélyek magánszférája és adatainak védelmét védő jogai sérelmére nem lehet alkalmazni.

**Webtracking**

17. A webtracking az egyén számos weboldalon megmutatkozó online viselkedésére vonatkozó adatok sütikkel, a JavaScript-tel vagy gépi ujjlenyomatok bármely formájával *[az egyén azonosítása az által használt technikai eszközök jellemzői, pl. a böngésző-beállításai segítségével]* való gyűjtése, majd ezt követő rögzítése, felhasználása vagy megosztása. A webtracking technológiák a felhasználóra vonatkozó, olyan valós idejű információk folyamatos áramlását teszik lehetővé, mint például a regisztrációs adatok, az online keresési adatok, viselkedési adatok, a felkeresett weboldalak adatai és konverziós adatok *[vásárlás során kattintással jelzett adatváltás]*, amelyek azt tükrözik, hogyan reagált a fogyasztó az egyedi ajánlatra. Ezeket az adatokat fel lehet dolgozni abból a célból, hogy értékeljék, valamiféleképpen kezeljék vagy befolyásolják az egyén állapotát vagy magatartását. Az egyéni viselkedést jellemző adatokon alapuló ügyfélprofil üzleti döntésekhez vezethet. A potenciális ügyfél értéke összefüggésbe hozható azzal a lehetőséggel, hogy őt adott áru megvásárlására késztessék.

18. A webtracking technológia jelen van a mobil eszközökön. Nagyon is valószínű, hogy a magánszemélyek nem cserélik egymás között intelligens, „smart" mobil eszközeiket, ezért a készülék és a magánszemély közötti kapcsolat szorosabb, mint például az ember és az asztali számítógép között. A mobil eszközök olyan egyértelmű eszközazonosítókat tartalmaznak, mint például a reklámspecifikus azonosítók,[17] az egyedi eszköz azonosítók (UDID) *[egyértelmű, géppel olvasható jelzet]*, a MAC-címek (Media Access Control) *[például minden egyes hálózati adapter hardvercíme]*, a Bluetooth MAC-címek, az NFC MAC-címek (Near Field Communications) *[a kistávolságú adatátvitel nemzetközi szabványa]*, az International Mobile Subscriber Identifier (IMSI, egyedi SIM-kártyaszám) és az International Mobile Equipment Identifier (IMEI) *[a mobileszköz egyedi sorozatszáma]*. Ezeket az azonosítókat a felhasználó általában nem tudja megváltoztatni. Az egyedi azonosítókon túlmenően az intelligens mobil eszközök rengeteg egyéb, olyan adatot is tartalmazhatnak,

---

és e gyakorlat alapján, ha szükséges, automatizálják a döntéshozást. Így a felhasználóknak nem kell minden, felkeresett oldal adatvédelmi szabályzatát elolvasniuk. URL: http://www.w3.org/P3P/.

[16] Omma Global Measurement 3.0, URL: http://www.webmetricsguru.com/archives/2008/09/measurement-30-on-the-next-5-years-omma-global-day-2/.

[17] A reklámspecifikus azonosítók lehetővé teszik annak korlátozását, hogy egy felhasználó hányszor látott egy reklámot, a viselkedési reklámok beillesztését, egy reklámkampány kiterjedésének és hatékonyságának mérését.

mint például a felhasználó neve, jelszava, kora, neme és címjegyzéke. Ezek az eszközök pontos viselkedés-specifikus adatokat jeleníthetnek meg. A helymeghatározó adatok au intelligens mobil eszközökön minden további nélkül rendelkezésre állnak.

19. A webtracking technológia különféle módokon alkalmazható. Egy digitális adatnyomvonal az adatok nem szándékos és akaratlan felfedéséből adódhat, ami (személyes) adatok szükségtelen felfedéséhez vezethet. Egy digitális adatnyomvonal sokféleképpen generálható. Egy digitális reklám kampány-menedzsere például egyedi azonosítót rendelhet a felhasználóhoz, a böngészőhöz vagy az eszközhöz. Másik lehetőség a terelő információk egyediesítése a célcsoport-információk (mikroprofil) hozzáadásával, melynek révén más, a reklámkampányban résztvevő weboldalak, a felhasználó, a böngésző vagy az eszköz ugyancsak nyomon követhető. Egy harmadik példa az egyedi azonosítók korrelációja egy meghatározott weboldal korábbi felkeresésekor gyűjtött adatokkal. Egy negyedik példa, amikor egy reklámkampány nyomkövetése újabb nyomkövető adatoknak (egy felhasználó, egy böngésző vagy egy eszköz adatainak) egy, korábban egy meghatározott weboldalon gyűjtött adatokkal vagy más harmadik féltől nyert adatok kombinációjával folyik. Végül egy utolsó példa a Cookie Matching-Services *[szolgáltatás, amely egy felkeresett weboldal sütijeit a felhasználó számítógépén tárolt sütikhez illeszti]* felhasználása, amely az internet különböző részei felhasználásával ugyanannak a felhasználónak, böngészőnek vagy eszköznek a digitális nyomait köti össze.[18]

20. A webtracking több automatikus lépésből áll, kezdve a webadatok gyűjtésétől ezen adatok rögzítésén keresztül az adatok felhasználásáig. Az adatok újbóli kombinálásával, korrelálásával és környezetüktől való megfosztásával a webadatok az egyéni viselkedés nagyon pontos profilírozására és előrejelzésére használhatók fel. Végül a webtracking egy meghatározott személy profiljának tényleges felhasználásához vezet.[19]

21. Az adatok az Internet különféle szolgáltatásai által használt gráf-adatbázisokban tárolhatók.[20] A gráf struktúrája lehetővé teszi olyan viselkedési minták felfedezését, amelyek egyébként ismeretlenek maradnának. Webtracking-adatok egy gráfban a felhasználói viselkedésre vonatkozó jelentőségteljes mintákat generálhatnak önmagukban vagy egyéb, különféle forrásokból származó adatokkal kombinálva. Amíg például egyes egyedi azonosítók közvetlenül vagy közvetve egy felhasználóhoz kötődnek és bár csak csekély információt nyújtanak az alkalmi böngészőről, az egyedi azonosítók gyűjtésével mélyre ható bepillantáshoz jutunk egy személy Interneten való szokásaiba és böngészési viselkedésébe. Az egyértelmű azonosítók gyűjtése egy digitális azonosság képzésére használható.

**Webtracking és az egyén magánszférájának és adatainak védelméhez fűződő joga.**

22. A nemzetközi jogszabályok széles körének alapelve az Internet felhasználói magánszférájának a technológiától független védelme. A kulcsfontosságú elemek: átláthatóság, ellenőrzés és a kontextus figyelembe vétele. Az a tény, hogy a felhasználók nincsenek tudatában annak, hogy nyomaikat követik, adatvédelmi kockázatot jelent. A webtracking mint folyamat egy sor olyan technikai eszközt alkalmaz, melyek a felhasználó

[18] Lásd például: https://developers.google.com/ad-exchange/rtb/cookie-guide#what-is.

[19] Lásd ugyancsak: Recommendation CM/Rec(2010)13 of the Council of Europe on the protection of individuals with regard to automatic processing of personal data in the context of profiling. (Az Európa Tanács ajánlása az egyének személyes adatainak a profilalkotás céljából való automatikus feldolgozása során való védelmére.)

[20] A gráf, a gráfelmélet alapvető fogalma, a dolgok (csomópontok, csúcsok) és a rajtuk értelmezett összeköttetések (élek) halmaza. Az értelmezések a csomópontokra és csúcsokra vonatkozó metainformációt tartalmazhatnak.

tájékoztatásának lehetőségét korlátozzák. Például a pixelek (pl. Web-Beacons) és mini-web-oldalak (pl. iFrames) az emberi szemnek láthatatlanok, egy weboldalba való befoglalásuk automatikus HTTP-igényt kezdeményez, ideértve egyedi azonosítókat tartalmazó sütik beültetését és a hozzáférhetőségüket.

23. Sok webtracking technológiát fejlesztett ki és alkalmazott a gazdaság anélkül, hogy tájékoztatta volna a felhasználókat adataik gyűjtéséről és anélkül, hogy választási lehetőséget kínált volna nekik. Azoknak a felhasználóknak a jelentéseit, akik a nyomkövetés elutasítására igényt formáltak, nem vették figyelembe, és néhány nyomkövetési módszer elleni technikai megoldást aktívan megkerültek, például a törölt sütik újbóli beillesztésével, (passzív) ujjlenyomattal és a böngésző beállítások megkerülésével. Csak amikor erre a magatartásra fény derült, és azt nyilvánosan kritizálták, vették tudomásul a felhasználó szabad akaratának tiszteletben tartására vonatkozó kötelességüket az érdekelt felek. Ilyen esetekben olykor opt-out programokat alkalmaztak, amelyek azonban a felhasználónak gyakran csekély haszonnal járó ügyetlen mechanizmusoknak bizonyultak. Ezek az esetek megrengették a felhasználóknak az Internet-szolgáltatók iránt táplált bizalmát és őszinteségükbe vetett hitét, és aláásták az innovatív Internet-szolgáltatások egészséges fejlődését.

24. A webtracking sok jogrendszerben személyes adatok feldolgozását jelenti, éspedig annak a ténynek az alapján, hogy a technológia lehetővé teszi a felhasználók individualizálását és azonosítását[21], valamint a rájuk vonatkozó automatikus döntések meghozását. Egy ilyen gyakorlatra például szolgálhatnak a valós idejű algoritmusokkal automatikus döntéseket hozó gépek, mely döntések alapja az egyéniesített viselkedési reklámra válaszul adott ajánlat.

25. Néhány érdekcsoport nagy ellenállást tanúsít az egyértelmű azonosítóknak a web-adatok mint személyes információk közé való besorolása ellen. Egy gyakran ismételt kijelentés szerint ezek az adatok, mihelyt anonimizálták őket[22], már nem személyes adatok. Mindazonáltal világos, hogy egy „célhoz kötött" elem felelős lehet azért, hogy az információk egy meghatározott személyre „vonatkoznak" vagy ezt a személyt érintheti.[23]

A „Ne kövess" lehetséges hatása (vagy hatásának hiánya) – esettanulmány

26. 2011 szeptemberében a W3C megalapította a Tracking Protection Working Group-ot[24] *[Munkacsoport a Webtracking elleni Védelemre].* A csoport egy Do-Not-Track Standard-en (DNT) dolgozik. Bár minden jelentős böngésző-fejlesztő kötelezettséget vállalt arra, hogy a sztandardot alkalmazza (és a többségük már annak megfelelően alkalmazta is a HTTP-fejlécet), mindazonáltal azok között az érdekcsoportok között, akik figyelembe fogják venni a DNT:1 Request-et[25], nyilvános vita folyik az önkéntesen alkalmazandó standard egyes

[21] Az általános adatvédelmi irányelv (95/46/EC) indokolásának 26. bekezdése szerint: „mivel a védelem elveit minden azonosított vagy azonosítható személyre vonatkozó információ esetében alkalmazni kell; mivel annak meghatározására, hogy egy személy azonosítható-e, minden olyan módszert figyelembe kell venni, amit az adatkezelő, vagy más személy valószínűleg felhasználna az említett személy azonosítására; **http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:hu:HTML**.

[22] Az anonimizálást azt jelenti, hogy az adatokat törlik modosítják, kumulálják, azonosítúiktól megfosztják vagy más módon manipulálják.

[23] 4/2007 vélemény a személyes adat fogalmáról (WP136), 10. oldal. **http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2007_en.htm**.

[24] A Munkacsoport küldetése a felhasználó magánszférája védelmének és a felhasználó ellenőrzési lehetőségének fokozása olyan mechanizmusok segítségével, amelyek a felhasználó preferenciáit figyelembe véve blokkolják vagy megengedik a web tracking elemek használatát. URL: **http://www.w3.org/2011/tracking-protection/charter**.

[25] A DNT sztandard jelenlegi tervezete szerint egy „0" küldése azt jelzi, hogy a tracking rendben van, míg egy „1" azt a tracking elutasítását jelzi.

részeiről. Néhány érdekcsoport úgy nyilatkozott, hogy a DNT-jelzést nem szándékoznak figyelembe venni. A DNT átfogó sikere a DNT-jelzésnek az azt fogadó szervezetek által való tényleges figyelembe vételétől és a DNT standardnak a Interneten való teljes, valamennyi érdekcsoport általi elfogadásától függ.

27. A DNT alapértelmezett beállításai és a webtracking szervezetek alapértelmezett akciói mindazonáltal rendkívül fontosak maradnak. Hogy a DNT a felhasználó ellenőrzési lehetőségeinek megvalósítására szolgáló hatékony eszköz legyen, az azért rendkívül fontos, hogy a webtracking alkalmazói is biztosítva legyenek arról, hogy az általuk fogadott DNT-jelzés a felhasználó kívánságának valódi megjelenítése. Ha a felhasználó egy ilyen választási lehetőségről részletes tájékoztatást nem kapott, a webtracking szervezetnek abból az alapértelmezésből, vagyis – mintha megkapta volna – abból a DNT:1 jelzésből kell kiindulnia, amely a felhasználónak azt az akaratát jelzi, hogy a trackinget nem kívánja.

28. Minden, a webtracking céljaira használt technológiának arányosnak kell lennie. A világszerte alkalmazott adatvédelmi elvek arra a feltevésre épülnek, hogy az adatok meghatározott, félreérthetetlen és jogszerű célokra gyűjthetők, és nem dolgozhatók fel oly módon, ami e célokkal összeegyeztethetetlen. Az adatok feldolgozásának megfelelőnek és lényegesnek, a feldolgozásnak az adatok gyűjtése és/vagy további feldolgozása céljához illeszkedőnek kell lennie.

29. Végül minden technológiának a bíróság előtt is meg kell állnia a helyét, ha hozzá akar járulni a magánszféra védelméhez. A DNT azzal a veszéllyel jár, hogy egy olyan szerszám marad, amely az információs társadalomban egy felhasználónak a szolgáltatóval szembeni kívánságát fejezi ki anélkül, hogy az egy konstruktív párbeszéd hatékony eszköze lenne. Ez a felhasználót magát vagy bármely olyan közjogi (vagy magánjogi) testületet, amely ilyen kívánságok vagy szabályok (ide értve egy egyedi személy jogi kötelezettségeinek figyelembe vételét is) a megfelelő jogi kötelezettségek alkalmazásával van megbízva, üres kézzel hagyja egy ilyen szolgáltatóval szemben. A gazdaság egyes érdekképviseleti csoportjai megpróbálják azt az álláspontot védeni, hogy a DNT nem jelenti egy kívánság figyelembe vételének kötelezettségét. Ámbár ez az értelmezés több, mint kétséges, az a tény változatlanul fennmarad, hogy nehéz bizonyítani, vajon egy ilyen kívánságot figyelembe vettek-e vagy nem.[26] Más szóval: kikényszerítésének perspektívájából ítélve a DNT egy placebó, s nem egy hatékony segédeszköz marad, s mint ilyen, haszontalanná válik.

**Javaslatok.**

30. A nem ellenőrzött webtracking megváltoztathatja a szolgáltató és az egyének közötti egyensúlyt, méghozzá a magánszféra védelmére való tekintettel is. A Munkacsoport hangsúlyozza, hogy a kontextus, az átláthatóság és az ellenőrzés kulcsfontosságú elemek maradnak a webtracking környezetben is.

31. A munkacsoport – az egyén magánszférája védelmét veszélyeztető kockázatok csökkentéséhez való hozzájárulásként – a következő ajánlásokat teszi a különböző érdekcsoportok részére, melyek a webtracking ökorendszerében szerepet játszanak.

**A személyes adatok bármely felhasználása esetére alkalmazzuk ismét a kontextusra és a célhoz kötöttségre vonatkozó alapvető elveket:**

[26] A külső audit fontos szerepet játszhat a fentebb körülírt probléma legalább részleges kezelésében, de másrészről tovább fokozza az ökorendszer bonyolult voltát.

– elővigyázatossági szempontok beépítése bármely adatgyűjtési, adatfeldolgozási vagy adatcsere gyakorlatba oly módon, hogy a valamely kontextusban gyűjtött adatokat ne lehessen felhasználni egy másik kontextusban;
és
– tájékoztatás az adatgyűjtés céljáról annak megkezdése előtt, és a cél változatlanul hagyása, hacsak a változtatást újabb tájékoztatás és választási lehetőség nem követi.

**Állítsuk vissza az átláthatóságot:**
Ne alkalmazzunk átláthatatlan elemeket;
– a felhasználó számára érthetően fogalmazott formában adjunk tájékoztatást arról, ha az alkalmazási program képes arra, hogy webtracking-jelzést küldjön a fogadó szerverre vagy ilyen jelzést az eredeti szerverről fogadjon;
– mindig adjunk a felhasználó számára feltűnő jelzést arról,[27] hogy egy webtrackingre éppen sor kerül;
– oly módon adjunk tájékoztatást arról, hogy egy webtracking éppen folyamatban van, hogy az különös felhasználói csoportok, ide értve a látáskorlátozottakat, rendelkezésére is álljon.

**Állítsuk vissza a felhasználó ellenőrzési lehetőségét:**
– alkalmazzunk olyan mechanizmusokat, amelyek lehetővé teszik, hogy a felhasználó a magánszférával és az adatvédelemmel kapcsolatos jogait az Interneten gyakorolja, és ne alkalmazzunk újabb tracking-módszereket, melyek a felhasználói ellenőrzést nem teszik lehetővé; amikor böngésző szoftvert installálunk, aktiválunk vagy aktualizálunk, tegyük lehetővé, hogy a felhasználó explicite megválaszthassa, kíván-e trackinget vagy nem;
– ha a böngésző nem rendelkezik felhasználói interfésszel, a szokásos beállításnak olyannak kell lennie, hogy a felhasználó nyomkövetésére (tracking) ne kerüljön sor;
– adjunk lehetőséget a felhasználónak arra, hogy választását eredeti döntését követően bármikor felülvizsgálja és a beállítást megváltoztassa; adjunk egyszerű lehetőséget a felhasználónak arra, hogy az (automatizált) választási lehetőségeket kipróbálja, és emlékeztessük őt arra, hogy a webtracking-re vonatkozó (automatizált) beállítást bármikor visszavonhatja, és biztosítsuk őt arról, hogy a választás technikailag egyszerűen, az egyénnek elviselhetetlen teher nélkül megvalósítható;
– vegyük figyelembe az alkalmazási programnak a trackinget elutasító jelzéseit;
– tartózkodjunk a (passzív) ujjlenyomattól, például a felhasználó által generált adatok (például a szolgáltatás konfigurációja vagy a böngészőt azonosító jelsorozatok */user agent strings/*) átkutatásától *[data mining]*, amely arra szolgálna, hogy egyedi felhasználó azonosítót származtassunk (device fingerprinting), amikor a felhasználó úgy nyilatkozott, hogy a tracking-et elutasítja;
– gondoskodjunk arról, hogy bármely új technológia alkalmazása abból a célból, hogy a felhasználónak választási lehetőséget nyújtson, kipróbálható, és azt az illetékes, a különféle jogrendszerekben rögzített rendelkezések végrehajtásával megbízott magánjogi vagy közjogi testület is felülvizsgálhassa, mely rendelkezések – világszerte számos jogrendszerben – a magánszemély magánszférája védelmének alapját képezik.

**********

[27] Különös figyelmet kell fordítani arra, hogy az Internet felhasználók egyetlen csoportját se kezeljük kevésbé előnyösen vagy különböztessük meg őket másképp, például fogyatékosságuk szerint.